INFLUECNING PRIVACY ON SOCIAL NETWORK SITES: HOW CONTEXTUAL CUES AND SURVEILLANCE PRIMES AFFECT DISCLOSURE BEHAVIOR AND PRIVACY SETTING DESCISIONS

A Dissertation

Presented to the Faculty of the Graduate School

Of Cornell University

In Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

By

Erin Lenore Spottswood

August 2014

ABSTRACT

INFLUECNING PRIVACY ON SOCIAL NETWORK SITES:

HOW CONTEXTUAL CUES AND SURVEILLANCE PRIMES AFFECT DISCLOSURE

BEHAVIOR AND PRIVACY SETTING DESCISIONS

Erin Lenore Spottswood, Ph. D.
Cornell University 2014

Nissenbaum's (2010) framework of contextual integrity contends that informational norms, which are characterized by key parameters or cues, indicate if a disclosure is appropriate to share in a given context. These cues include aspects of the context, relationship between interaction partners, attributes of the information being shared, and constraints on how information can be shared. Offline, these cues are relatively easy to identify, and help people locate and follow informational norms in their day-to-day lives. However, SNSs tend to obscure many of these cues, making it difficult for users to follow relevant informational norms on these sites. This study explored two factors that may affect participants' ability to abide by informational norms in SNS contexts. The first factor is a form of contextual cue that indicated how frequently other users had shared information on the site. The second factor is a class of primes called eye primes, in which the presence of eyes in one's visual field increases normative behavior in a wide range of settings (for review See Nettle et al., 2013).

Study 1 explored what kinds of information students evaluate as appropriate versus inappropriate to disclose on a university-affiliated SNS to get a baseline understanding of the informational norms students would apply to a specific kinds of SNS. Study 2 examined how contextual cues and eye primes affected disclosure behavior and found that the contextual cues affected disclosure behavior relative to when there were no cues present, but the eye primes only affected disclosure behavior when contextual cues were also present in this context. Study 3

explored how contextual cues and eye primes affect privacy setting decisions, and found that contextual cues affected how strict participants set their privacy settings. In addition, placing the privacy settings page before the profile page nudged participants to disclose more inappropriate information than when they filled out a profile before making privacy setting decisions.

The results of these three studies suggest that contextual cues and eye primes can affect information sharing behavior on SNSs. This not only has important implications for Nissenbaum's (2010) framework of contextual integrity but also has interesting implications for Brandimarte and colleagues (2013) privacy paradox as well.

BIOGRAPHICAL SKETCH

Erin Lenore Spottswood earned her Bachelor of Art's degree in Communication from Carthage College in Kenosha, Wisconsin. Prior to pursuing her doctoral degree at Cornell University, she received her Master of Arts degree in Communication from Michigan State University in East Lansing, Michigan. In 2010 she joined the doctoral program in Communication at Cornell University, and defended her dissertation in July 2014. After finishing her doctoral program, she joined the faculty at Portland State University as an Assistant Professor.

ACKNOWLEDGEMENTS

I would like to express deep and profound gratitude to my adviser and mentor, Professor Jeffrey T. Hancock, for his unwavering guidance, patience, and encouragement. Throughout my time at Cornell, he has helped me hone my skills as a meticulous researcher, an inspired teacher, and as a professional academic. My success is his success.

I would also like to thank Professors Natalie Bazarova, Lee Humphreys, and Melissa Ferguson for their inspiration and support. Professor Bazarova inspired me to strive for excellence, Professor Humphreys encouraged me to see the bigger picture, and Professor Ferguson helped me uncover how the conscious and unconscious intricately affect social behavior. They are more than my committee members; they are also my role models.

I would like to thank Dr. Lynn M. Johnson and Dr. Françoise Vermeylen for their keen and helpful guidance on data analyses for my projects. I would like to thank Scott Cambo for his amazing work on developing and operating the website and survey featured in my research.

I would like to thank Jessie Taft for her support, feedback, counsel, and editing. Not only was she a tremendous asset to this project, her friendship helped me push through time and time again.

Special thanks to Rachel Ellicott, Janice Park, and Carolyn Sussman for their help with project development, data collection, participant recruitment, and data analyses.

I would also like to thank my parents, my brother Mark and his wife Sarah, my twin sister Jayne as well as my dear friends Dr. Darren Le Puigh, Dr. Mohammad Hamidian, Professor Christopher Carpenter, Joanna Alario, Romana Hamilton, and Mike Maffie for their affection, counsel, and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

How do people decide when and when not to disclose their private information on Social Networking Sites (SNSs)? Users often post private or sensitive information publicly on SNSs, perhaps because they don't take into account how and when other people can access their information on these sites (Acquisti & Gross, 2009). This is likely because SNSs are a context that obfuscates the norms that indicate what kinds of information that are appropriate to disclose on these sites. Informational norms prescribe what kinds of information are appropriate to disclose in a variety of contexts (Nissenbaum, 2010; 2011). Nissenbaum posits that people use these norms to assess the appropriateness of disclosure behavior both offline and online. However, given the multi-faceted nature of SNSs, deciphering and following such norms can be a challenging process, leaving many users to inadvertently violate their own and other users' privacy (Litt et al., 2014).

This dissertation will examine how users can be made aware of and influence if they will follow informational norms on SNSs. First I draw on Nissenbaum's (2010) framework of contextual integrity and use it as a framework to explain how increasing the salience of norms on SNSs might influence user disclosure behavior and privacy setting decisions. In order to test this premise, Study 1 surveys what kinds of information university students feel are appropriate to disclose on a university-affiliated SNS to establish the informational norms users apply to this context. Study 2 will draw on the results from Study 1 and explore two factors that may affect how frequently and how accurately users disclose information in this context. The first factor is a form of contextual cue which makes users aware of how frequently other users have shared information on the site. Will providing this kind of contextual cues modify user behavior by making informational norms more salient? The second factor is a class of primes called eye

primes, in which the presence of eyes in one's visual field increases normative behavior in a wide range of settings (for review see Nettle et al., 2013). Considering that SNS informational norms influence the likelihood that users will disclose accurate information on their profiles (Ellison, Hancock, & Toma, 2012; Young & Quan-Haase, 2009), could eye primes not only push users to disclose more frequently but also more accurately on their own and when coupled with contextual cues?

Study 3 extends this analysis to privacy setting decisions, such as choosing more open or strict privacy settings. Users sometimes model their privacy setting decisions on their friends' decisions on privacy settings (Utz & Krämer, 2009), suggesting that users may also draw on contextual cues that indicate what other users have done regarding privacy settings. Study 3, therefore, examines whether contextual cues and eye primes affect privacy setting decisions on a SNS.

Privacy

Over the years, the notion of privacy has evolved from general beliefs about what privacy is to how people manage their privacy via disclosure behaviors. According to Altman (1975), privacy is perceived as an "interpersonal boundary process by which a person or group regulates interaction with others" (p. 6, italics in original). Margulis (1977) expanded upon Altman's (1975) conception of privacy by emphasizing the importance of control; "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability." (p. 10). Derlega and Chaikin (1977) take Margulis' (1977) definition of privacy a step further by emphasizing how disclosure behavior can affect people's ability to exert control over their privacy. According to Derlega and Chaikin (1977) self-disclosure is defined as "the verbal transmission of information about

oneself" (p. 103), while personal or sensitive information is defined as information that focuses on "aspects of the self that are unique or central and/or vulnerable, such as personal inadequacies, one's sexual life, or special goals" (p. 104). When a person discloses sensitive information, they give the recipient the ability to share that information with others, meaning disclosing sensitive information is synonymous with relinquishing a certain amount of control over their privacy.

Theories that address privacy behaviors have emerged alongside the evolution of the conceptualization of privacy. In communication contexts two important theories that focus on privacy include Petronio's (2002) Communication Privacy Management Theory (CPM), which offers insight into how people manage their privacy in various contexts, and Nissenbaum's (2010) framework of Contextual Integrity.

Petronio's (2002) CPM theory is comprised of 5 overarching principles that describe how people manage their privacy and exert control over their sensitive information in various contexts. The first principle posits that people believe they own their information. The second principle posits that people feel they have a right to control how their information is shared with others. The third principle posits that people use privacy rules to decide whether they should disclose or conceal different kinds of information. The fourth principle posits that recipients of information should abide by relevant privacy rules or negotiate new rules. The fifth principle posits that sometimes privacy rules are broken and result in boundary turbulence.

The third principle is particularly important because it sheds light on the disclosure decision process. According to Petronio (2002), people use privacy rules to determine when, where, and with whom they should disclose sensitive information. People acquire these rules via socialization and routinization processes. Socialized privacy rules are often learned by

interacting with members of a social group. For example, she describes how children are socialized to learn their families' privacy rules that indicate what kinds of information should not be disclosed with non-family members (p. 72-75). Routinized privacy rules are learned by habitually following a privacy rule in a given context. For example, she highlights how people typically do not discuss their finances with strangers because they are discouraged from doing so early on in life.

Although the CPM explains how privacy rules are acquired, it does not delve into how these rules are determined and applied, making it difficult to determine how these rules can be used to make disclosure decisions. For example, parents may teach their children not to disclose information about their family's health issues with non-family members because said information has very sensitive attributes. This suggests that children must identify whether or not an interaction partner is a family member in order to determine if they can discuss their sister's illness openly with another person. In other words, children can use cues about an interaction partner (i.e., whether or not they are a family member) to determine if they can discuss their sister's illness without violating their family's privacy rule.

In contrast to the CPM theory's assumptions about how disclosers infer and apply privacy rules to various contexts, Nissenbaum's (2010) framework of contextual integrity focuses on how people use contextual cues to infer a context's privacy rules, which in turn helps them determine if it is appropriate to disclose sensitive information in a given context. The central tenet of Nissenbaum's (2010; 2011) framework of contextual integrity is that all social situations are denoted by key characteristics that give cues about how to behave appropriately in a context. Contexts are defined as structured social settings characterized by *canonical activities, roles, relationships, power structures, norms* (or rules), and *internal values* (Nissenbaum, 2010).

For example, a university is a context with specific canonical activities, such as taking exams and lecturing in classrooms, that are carried out by individuals in specific roles and relationships (e.g., student-professor, advisor-advisee), situated within a power structures in which professors hold power over students, deans hold power over professors. These contexts are endowed with a rich set of norms that prescribe certain behaviors and proscribe others. For example, it is not appropriate to answer calls during a lecture because it violates norms endowed to this particular canonical activity, namely that students pay attention during class, as well as power structures, in this case taking a call is an affront to the professor's authority in the classroom.

One type of norm that is particularly important to privacy and is therefore central to Nissenbaum's framework is *informational norms* that specifically prescribe what kinds of information are appropriate to disclose in a context. Informational norms can be determined by four key parameters: *contexts, actors, attributes, and transmission principles* (Nissenbaum, 2010). Contexts are "abstract representations of social structures experienced in daily life" (p. 134). According to Nissenbaum (2010), informational norms that are firmly established in a context prescribe what kinds of information are appropriate to disclose in that context. This should apply not just for a specific context, such as a particular university, but across contexts that are of a similar type (i.e., universities in general). For example, entrenched university norms prescribe that students should be careful where and with whom they disclose information regarding their health and well-being. A student may want to explain to their professor that they've missed several classes due to illness in order to preserve their relationship with the professor as well as their grade in that class. However, entrenched university norms prescribe that it is more appropriate to disclose such information in the professor's office than during a lecture so the student can avoid revealing their illness to unwarranted third parties (e.g., other

students, teaching assistants, etc.). Given that this is an entrenched norm, university students should abide by this regardless of which specific university they attend.

Attributes refer to the nature of the information being disclosed (Nissenbaum, 2010, p. 143). Attributes can include how sensitive, personal, and private a piece of information is. For example, sensitive information typically contains attributes that can identify the discloser as well as leave the discloser feeling vulnerable (Derlega & Chaikin, 1977). Sensitive information tends to be perceived as inappropriate to disclose in public contexts with non-close recipients because the discloser cannot be certain recipients will protect or respect their sensitive information. For example, the truth about why a student has been absent from class (e.g., they were not ill but actually on a Caribbean Cruise) is a piece of information with relatively sensitive attributes given that it can make the student vulnerable to social and academic sanctions (e.g., fail the course). As a result, the student likely believes that it would be inappropriate to disclose about his trip in a public or crowded context because he cannot ensure his sensitive disclosure will not be overheard and subsequently shared with his professor.

Actors are the senders, receivers, and information subjects within a context (Nissenbaum, 2010). Actors are another cue that helps determine whether or not it is appropriate to disclose specific kinds of information in a given context. For example, it is appropriate for a student to tell a close friend that the real reason they've been absent was that they were on a Caribbean cruise because the close friend can be trusted not to reveal their sensitive disclosure to others. It is not appropriate to disclose the same information to a teaching assistant because the assistant is an authority figure expected to disclose information about a student's whereabouts with the professor.

Finally, transmission principles place constraints on the distribution and dissemination of private information from party to party within a context, prescribing when a transfer of information is appropriate (Nissenbaum, 2010). For example, the truth about a student's absence from class is private information given its incriminating attributes. If that information was disclosed with a friend, transmission principles dictate that is it inappropriate for the friend to transmit or disclose that piece of information with any other actor unless designated by the student himself. According to the framework of contextual integrity (Nissenbaum, 2010), the sharing of private information must take into consideration some or all of these factors in order to determine the appropriateness of a disclosure.

Nissenbaum's (2010) framework of contextual integrity can be used to explain whether information disclosures are appropriate or not (Archer & Berg, 1978; Chaikin & Derlega, 1974; Wortman, Adesman, Herman, & Greenberg, 1976). For example, Chaikin and Derlega (1974) expected their participants to judge the appropriateness of a disclosure according to how well the discloser knows the receiver: sensitive disclosures to a close friend should be judged as most appropriate, sensitive disclosures to an acquaintance should be judged as less appropriate, and sensitive disclosures to a stranger should be judged as least appropriate. This is consistent with Nissenbaum's (2010) framework of contextual integrity that posits people should rate the appropriateness of a sensitive disclosure according to the actor and relational factors attributed to conversation partners (i.e., it is appropriate for close friends to disclose sensitive information with each other). Consistent with their expectations, Chaikin and Derlega (1974) found that sensitive disclosures to anyone other than a close friend were judged as inappropriate, and the discloser was judged as socially undesirable. This suggests that not only do people find sensitive disclosures inappropriate when disclosed with a non-close actor, but that those who violate this

norm may incur social sanctions. These results are consistent with Nissenbaum's (2010) assertion that contextual cues can affect whether or not a disclosure is considered appropriate, and can help a person determine whether or not they should disclose sensitive information during a FtF interaction.

More recent research has also examined how users evaluate other users' disclosures on Facebook (Bazarova, 2012), and demonstrates how contextual cues can affect appropriateness evaluations in SNS contexts. For example, Bazarova (2012) examined how entrenched FtF norms condemning sensitive disclosures in public contexts apply to the SNS Facebook. Sensitive disclosures were expected to be perceived as inappropriate when disclosed publicly, and that participants would be less socially attracted to a sender who made inappropriate public disclosures. She found that highly sensitive, negative valence disclosures were rated as less appropriate when presented on public walls than when they were presented as private messages, and that posting these messages on a public wall decreased participants' social attraction for the sender.

These results suggest that the contextual cue of publicness influences appropriateness evaluations of sensitive disclosures and disclosers on SNSs. However, it is unclear what other kinds of contextual cues might affect how users evaluate the appropriateness of disclosures on SNSs. For example, if Bazarova (2012) instructed participants to imagine the sender was a close friend, would they have rated the positive-sensitive messages as more appropriate, or rated the discloser as more likable, when those messages were disclosed publicly rather than privately?

One of the reasons why it is difficult to examine contextual cues and their effect on perceived appropriateness on SNSs is because the contextual cues necessary to make these evaluations tend to be obscured. SNS norms are difficult to decipher; they are not formally

documented, and they are not formally agreed upon by the user community (Hooper & Kalidas, 2012). In addition, SNS features often obscure the contextual cues that would make informational norms more salient in other contexts. For example, Facebook's "Friending" (Ellison, Steinfield, & Lampe, 2011) and default public communication (boyd & Marwick, 2011) features obscure which actors can access a user's disclosures, making it difficult for the user to determine whether their disclosures will be perceived as appropriate by other users on the site.

Privacy setting decisions can also affect whether participants adhere to a SNS's information norms. While users tend to perceive that selecting strict settings gives them control over who can see the content they post or disclose on a SNS (Liu, Gummadi, Krishnamurthy, & Mislove, 2011), this increased feeling of control can paradoxically increase the likelihood that a user will disclose sensitive information online (Brandimarte, Acquisti, & Loewenstein, 2013). Without the relevant cues, users may not be able to determine what kinds of information and which privacy settings they should select in order to conform to a SNS's informational norms. As a result, they may share information that is inappropriate (i.e., too sensitive) according to the site's user community, resulting in embarrassment and social sanctions (Litt et al., 2014; McLaughlin & Vitak, 2012; Wang et al., 2011).

While it may prove difficult to present users with all the relevant cues necessary for them to infer what is appropriate to disclose on a SNS, can contextual cues that indicate a site's informational norms affect disclosure behavior on the site? To address how providing contextual cues about information sharing norms affects disclosure behavior, it is important to first determine which types of information (e.g., age, address.) are perceived as sensitive and therefore inappropriate to disclose on a SNS.

Study 1 – Ascertaining Informational Norms on a SNS

The ways in which people traditionally discern informational norms in a context is by deciphering the relevant cues within that context (Nissenbaum, 2010). Even though contextual cues tend to be obfuscated in SNSs, users still have basic assumptions about what is appropriate to disclose publicly versus privately on a SNS (Bazarova, 2012). Moreover, SNS users might make assumptions about what is appropriate to disclose on a SNS according to other salient cues on the site. For example, given Facebook's labeling a user's network as their "Friends" list, users might interpret the word friend as a cue that the site is socially oriented. As a result, a user may perceive sensitive information such as pictures of their vacation as appropriate to disclose on the site.

Depicting a SNS as affiliated with a university might shift what students enrolled at that university perceive as appropriate to disclose on that specific SNS. For example, a university student may perceive disclosing their major/field of study as appropriate to disclose on the site because it does not contain sensitive attributes, suggesting it can safely disclosed with various members of a university (e.g., friends, classmates, professors, staff, etc.). However, a university student would likely perceive disclosing their past medical or health issues as inappropriate to disclose on the site because said information can result in social ramifications if shared with non-close others (e.g., ridicule) as well as authority figures (e.g., perceived as unfit to attend university). In summary, university students might evaluate information that contains sensitive attributes as inappropriate to disclose on a university-affiliated SNS.

While we might expect university students to use information attributes to help them evaluate the appropriateness of different kinds of information, there is no research to date that has explicitly examined what kinds of information university students evaluate as appropriate to

disclose on a university-affiliated SNS. As a result, Study 1 will investigate what kinds of information university students evaluate as appropriate to disclose on a university-affiliated SNS:

RQ1: What kinds of information do university students perceive as appropriate to disclose on a profile for a university-affiliated SNS?

Methods

Pilot Study. To develop an initial set of profile disclosure items, 10 undergraduate assistants from a Northeastern university (i.e., Cornell) were asked to list three pieces of information they perceive as appropriate to disclose on a profile for a university-affiliated SNS, three pieces of information they perceive as inappropriate to disclose on a profile for a university-affiliated SNS, and three pieces of information they perceive as appropriate to disclose on a profile for a university-affiliated SNS so long as they could control who could access their profile. These initial lists were combined, edited for redundancies, and used to develop the survey for Study 1.

Participants. Cornell undergraduate students were recruited to participate in an online survey. Participants were required to be over the age of 18 and enrolled at Cornell to be eligible for participation. There were a total of 44 participants who completed the survey.

Materials and Procedure. The survey asked participants to rate 42 different pieces of information according to how 1) how appropriate it would be to disclose that piece of information on a profile for a university-affiliated SNS, 2) how comfortable they would be sharing that piece of information on a profile for a university-affiliated SNS, 3) how private they perceive that piece of information to be, and 4) how sensitive they perceive that piece of information to be (Appendix A). Each item ranged on a scale from 1 (very inappropriate, extremely sensitive, etc.) to 5 (totally appropriate, not at all sensitive, etc.). After rating the

different kinds of information, participants were thanked for their time and awarded one research participation credit.

Results

The four questions (appropriateness, comfortableness, privateness, and sensitivity) had high reliability for each of the disclosure items, with Cronbach's *alphas* all higher than 0.76 (see Table 1). Factor analysis also revealed only one dimension from the four response items for all but one (i.e., fraternity/sorority) of the 42 information types, suggesting that the four response items were tapping one underlying factor.

The four items were averaged into a composite perceived appropriateness score for each of the 42 pieces of information. Lower mean scores indicated that participants perceived that piece of information as less appropriate to disclose on a university-affiliated SNS whereas higher mean scores indicated that participants perceived that piece of information as appropriate to disclose on a university-affiliated SNS (See Table 1). RQ1 asked if undergraduate students would differentially rate information according to how appropriate versus inappropriate they perceived it to be for this context. A frequency analysis of the appropriateness variable revealed that the data were normally distributed between the minimum (1) and maximum values (5), ($GM = 2.82$, $SD = 1.13$). In addition, 10 of the 42 information types were below the bottom quartile (1.86) and 9 of the 42 information types were above the top quartile (3.91).

Five disclosure items from the 25th percentile were selected for the inappropriate set of items, 8 disclosure items from the 50th percentile were selected for the somewhat appropriate group, and 5 disclosure items from the 75th percentile were selected for the appropriate group. As expected, the inappropriate, somewhat appropriate, and appropriate group means were significantly different from each other, $F(1, 42) = 1700.00$, $p < 0.001$ (see Table 2). These results

were used to develop the disclosure items in Study 2, and the final list of information asked for in Study 2 is displayed in Table 3.

Discussion

The results of Study 1 reveal what kinds of information specific actors, in this case students, perceive as appropriate to disclose in the specific context of a university-affiliated SNS profile. These results are consistent with Nissenbaum's (2010) contention that actors evaluate what kinds of information are appropriate to disclose in a context according to information attributes. Sensitive information can include identifiable (e.g., social security number) and very personal (e.g., past medical or health issues) attributes that are perceived as appropriate to disclose in private contexts with close others (i.e., people they can trust to protect their sensitive information), but are perceived as inappropriate to disclose in public contexts amidst non-close others (Greene, Derlega, & Matthews, 2006). This suggests that SNS users should refrain from disclosing information with sensitive attributes on their profile because SNSs profiles tend to be relatively public and will likely be seen and accessed by non-close (i.e., untrustworthy) others on the site.

The participants in Study 1 evaluated information with sensitive attributes as inappropriate to disclose in this context, likely because they expected their profile would be seen and accessed by those they cannot trust to protect or respect their sensitive information. For example, all of the information types from the inappropriate group contain sensitive attributes that could make the discloser vulnerable to identity theft (e.g., social security number, banking information) or public embarrassment (e.g., medical information, relationship history, etc.). As a result, participants likely perceived these information types were too sensitive to share on a SNS profile, which is why they also evaluated these information types as inappropriate to disclose in

this context. In contrast, participants evaluated information with less sensitive attributes (e.g., college affiliation, academic major, etc.) as appropriate to disclose in this context. In summary, students perceived information with sensitive attributes as inappropriate to disclose on a university-affiliated SNS. This supports Nissenbaum's (2010) basic contention that information attributes influences information appropriateness evaluations in various contexts.

Findings from Study 1 demonstrate that students evaluate information with especially sensitive attributes as inappropriate to disclose in a university-affiliated SNS context. As a result, we can expect that users will perceive information with sensitive attributes as inappropriate for this context, and refrain from disclosing sensitive or rather inappropriate information in this context. Using the appropriateness evaluations from Study 1 as a baseline, Study 2 examines how contextual cues and eye primes can affect how frequently and how accurately users disclose information that ranges in appropriateness in this context.

Study 2 – Influencing Disclosure Behavior

According to Nissenbaum (2010), people rely on informational norms to determine what is appropriate to disclose in a context. However, SNSs tend to obscure important contextual cues, undermining a user's ability to discern whether the type, amount, or accuracy of their disclosure is appropriate to disclose on the site. Instead, users tend to disclose in accordance with entrenched norms (i.e., norms that persist across similar contexts), at times violating their own or others' privacy. Can contextual cues that indicate disclosure norms (e.g., most users do not disclose their medical information) modify people's disclosure behavior and adherence to entrenched norms? This study examines how contextual cues and eye primes can affect disclosure frequency and accuracy on SNSs.

Entrenched Norms

Several studies find that Facebook users disclose relatively high amounts of information on their profiles (Christofides, Muise, & Desmarais, 2011; Lampe, Ellison, & Steinfield, 2007; Tufekci, 2008; Young & Quan-Haase, 2009), suggesting that the entrenched norm for self-disclosure on SNSs is to disclose high levels of information. For example, Lampe and colleagues (2007) found that Facebook users complete 59% of their profile, and in some fields display "a significant amount of information" (p. 440). This consistent pattern of results suggests that users habitually disclose a high level of information on SNS profiles. Moreover, the amount of information users disclose has increased in recent years (Madden et al., 2013; Stutzman, Gross, & Acquisti, 2013). This latter pattern of results suggests that as new users join SNSs, they disclose according to how previous users have disclosed on these sites. The staying power of this pattern of frequent disclosure suggests that users perceive that disclosing frequently is an entrenched norm in SNS contexts. In fact, users recognize that disclosing frequently is normative in SNS contexts; "why have a profile if your profile will not say *enough* about who you are?" (Tufekci, 2008, p. 33, italics in original).

As demonstrated in Study 1, however, users are more willing to disclose information that they perceive as appropriate more frequently than information that they perceive as inappropriate for SNS contexts (Bazarova, 2012; Bazarova, Taft, Choi, & Cosley, 2013; Hogan, 2010; Newman, Lauterbach, Munson, Resnick, & Morris, 2011; Qiu, Lin, Leung, & Tov, 2012; Young & Quan-Haase, 2009). For example, Newman and colleagues' (2011) interview subjects reported feeling that they should refrain from disclosing more detailed and personal accounts of their health struggles on Facebook's public communication features. Their reluctance to disclose their health struggles stemmed from their concern that most of their Facebook friends would perceive such disclosures as too sensitive and therefore inappropriate disclose in that context (i.e.,

Facebook). Another study found that not only do participants disclose less about their negative emotions on Facebook than they do offline, but perceive their friends do the same (Qiu et al., 2012). In other words, they perceived that negative emotions were too sensitive and therefore inappropriate to disclose publicly on Facebook in part because they perceived their friends refrain from disclosing similarly sensitive information on the site. These results suggest that SNSs contain entrenched norms that proscribe the public disclosure of more sensitive information (e.g., health struggles and negative emotions) on these sites.

Results from Study 1 reveal that users might apply similar appropriateness norms to a university-affiliated SNS context. In Study 1, participants evaluated sensitive information such as medical information and social security number as less appropriate than not sensitive information such as academic major and graduation year to disclose in this context. These evaluations echo the appropriateness findings from the studies discussed above. However, given the entrenched norm influences the likelihood that users will disclose information frequently; we expect that university students would disclose appropriate (i.e., less sensitive) information more frequently than inappropriate (i.e., sensitive) information in this context:

H1: Participants disclose inappropriate information less frequently than somewhat appropriate information, and disclose appropriate information most frequently.

Contextual Cues

Recent research has found that contextual cues that indicate norms about how frequently users disclose sensitive information can affect the likelihood that someone will disclose similar information in an online survey context. Acquisti and colleagues (2012) contend that disclosure behavior is comparative in nature; people can be nudged to disclose sensitive (e.g., having sexual desires for a minor) information if they perceive that a lot of other people have already disclosed sensitive information in the same context. To test this, they placed contextual cues on their

online survey that depicted how frequently other respondents had disclosed sensitive information. In other words, the contextual cue indicated a norm that prescribed whether participants should disclose sensitive information. The high cue indicated that most of the respondents disclosed sensitive information, while the low cue indicated that most of the respondents did not disclose sensitive information. A third condition included an omission cue that depicted most respondents had left the answer blank. Participants in the high cue condition were 27% more likely to disclose sensitive information relative to the low and missing conditions. This suggests that contextual cues that indicate disclosure norms can affect people's willingness to disclose information in a SNS context.

Based on this rationale, Study 2 tests the following predictions of the effect of contextual cues on disclosure behavior:

H2: Participants will provide the least information when low disclosure contextual cues are present and the most information when high disclosure contextual cues are present relative to when no contextual cues are present.

Eye Primes

Many studies in social psychology suggest that eye primes increase behaviors that are typically considered normative relative to the context (Bateson, Nettle, & Roberts, 2006; Ernest-Jones, Nettle, & Bateson, 2011; Haley & Fessler, 2005; Nettle, Harper, Kidson, Stone, Penton-Voak, & Bateson, 2013; Nettle, Nott, & Bateson, 2012; Rigdon, Ishii, Watabe, Kitayama, 2009) . Eye primes are images of eyes (drawing, picture, etc.) that, when placed in a person's field of view, can modify their behaviors. For example, eye primes can increase the likelihood that office workers pay for taking milk for coffee/tea out of their office break room (Bateson et al., 2006) and reduce littering in a university cafeteria (Ernest-Jones et al., 2011).

Eye primes have also been found to influence informational norms that prescribe politeness (Spottswood & Hancock, under review). In this study participants were asked to respond to scenarios in which a friend asked an awkward question, such as whether they had liked an awful meal that the friend had cooked, responding either via Facebook's public Timeline or private message communication features. After seeing their friend's public or private message, they were asked to pick the response that best resembled what they would actually say to their friend. The response choices were polite and deceptive (e.g., "The food was delicious, well done!") or impolite but honest ("You have to cut back on the salt."). Eye primes embedded into the ads that typically appear on the right hand side of Facebook's site pages had an important effect on whether participants followed politeness norms to avoid embarrassing their friend. In particular, eye primes increased the use of polite lies, suggesting that eye primes increase behaviors are consistent with informational norms relative to the context.

These results suggest eye primes have the capacity to increase behaviors that adhere to norms; however, it is unclear whether eye primes increase normative behaviors that are entrenched in a context or if they increase normative behaviors that are indicated by contextual cues. For example, Bateson and colleagues' (2006) featured eye primes on a contextual cue that indicated a norm prescribing people to pay for milk. However, the break room already contained an entrenched norm that also prescribed this behavior. This confounding of the entrenched norm with the indicated norm confuses the interpretation of their findings: did the eye primes increased how often people paid for their milk in accordance with the entrenched norm or in accordance with the indicated norm (contained in the contextual cue)? Another study examined how eye primes would affect another behavior entrenched to most outdoor contexts: bike theft. Nettle and colleagues (2012) "reasoned that" eye primes "could potentially be effective as part of an

intervention against the more serious norm violation of stealing a bicycle" (p. 2). To test this they featured eye primes on a contextual cue that indicated a norm proscribing bike theft at three bike racks at the researchers' university. They found that eye primes significantly reduced bike theft. However, the entrenched norm and the indicated norm contained in the contextual cue were similarly confounded, making it difficult to determine if the eye primes discouraged people from stealing bikes in accordance with the entrenched norm or in accordance with the indicated norm (contained in the contextual cue).

This study will attempt to tease apart this confound by making the norm indicated by the contextual cue different from the norm entrenched in this context. The contextual cues in this study will sometimes indicate that other users had disclosed sparingly on their profiles, suggesting an infrequent or low disclosure norm. This low cue will prescribe disclosure behaviors that run counter-intuitive to the entrenched norms that prescribe users to disclose frequently in SNS contexts. As a result, this study will explore whether eye primes affect norms indicated by contextual cues or affect norms that are entrenched in a context.

H3A: Eye primes increase adherence to contextual cues such that the difference between low and high disclosure contextual cues will be larger when eye primes are present than when they are not.
H3B: Eyes primes increase adherence to entrenched norms such that participants will disclose more information when the eye primes are present.

Accuracy

In addition to frequency, SNSs also have entrenched norms that influence another kind of disclosure behavior: accuracy. Accuracy is defined as the extent to which a disclosure is correct or true. A substantial amount of recent research suggests that SNSs have entrenched norms that encourage users to disclose accurate information on their profiles (Chen & Marcus, 2012; Ellison, Hancock, & Toma, 2012; Hancock & Toma, 2009; Hong, Tandoc, Kim, Kim, & Wise,

2012; Toma, Hancock, & Ellison, 2008; Young & Quan-Haase, 2009). These norms are in response to the ease with which users can engage in selective self-presentation on these sites (Toma et al., 2008). Users of online dating sites may be especially motivated to engage in selective self-presentation in order to maximize their dating success. For example, men tend to overreport their height by a few inches, whereas women tend to underreport their weight by a few pounds, in order to fit the physical ideal for their sex (Toma et al., 2008). These types of minor inaccuracies are not only accepted but are even expected by members of the online dating community (Ellison et al., 2012). However, inaccurately disclosing about marital or parental status is considered a serious norm violation because marital and parental statuses are crucial pieces of information for this community. If a user were to find out the single person they were pursuing actually had a spouse and children, they would likely feel hurt and alert other users about the deceptive user. In summary, dating site norms allow for minor inaccuracies, but accurate disclosures are generally perceived as more appropriate and expected than inaccurate disclosures in online dating contexts.

Similar to online dating sites, SNSs such as Facebook contain entrenched norms that influence the likelihood that users disclose accurate information on their profile and elsewhere on the site. Facebook users tend to disclose accurate information on their profiles (Hall & Pennington, 2013; Hong et al., 2012; Waggoner, Smith, & Collins, 2009; Weisbuch, Ivcevic, & Ambady, 2009; Young & Quan-Haase, 2013). In addition, a recent study suggests that Facebook users react more favorably towards users who have accurate profiles. Hong and colleagues (2012) had participants rate Facebook profiles with accompanying comments that were either congruent or incongruent with the information provided on the profile. Participants rated users with congruent or accurate profiles as more socially attractive, and more popular, than users with

incongruent or inaccurate profiles. Another study found that Facebook users are more likely to omit rather than inaccurately disclose information on their profiles in order to protect their privacy (Young & Quan-Haase, 2009). In fact, participants expressed that they were worried they would incur social sanctions if their friends and/or peers caught them disclosing inaccurate information on Facebook. These results suggest that users apply the entrenched SNS norm that influences disclosure accuracy on the SNS Facebook.

Accuracy has largely been overlooked in the SNS literature, which is unfortunate because it can demonstrate how users may try to adhere to frequency norms while simultaneously protecting their privacy. The SNS in the present study asks for SENSITIVE information that is typically considered as inappropriate on a SNS profiles (e.g., medical information). SNS users sometimes encode their public messages in order to protect their sensitive information in public SNS contexts (boyd, 2010; Madden et al., 2013; Papacharissi & Gibson, 2011; Raynes-Goldie, 2010). This suggests that users may resort to inaccurately disclosing inappropriate (i.e., sensitive) information in order to adhere to a frequency norm without actually violating their privacy. Therefore, participants may be more or less accurate depending on whether that piece of information's appropriateness level:

H4: Participants will disclose inappropriate information less accurately than somewhat appropriate information, and disclose appropriate information most accurately.

Contextual cues that indicate how frequently users disclose a piece of information should not influence accuracy. However, as discussed above, eye primes may be able to influence behaviors that are consistent with entrenched norms. Past research has shown that disclosing accurately is expected in SNS contexts (Toma et al., 2008) and that users tend to disclose accurate information on their profiles (Chen & Markus). These studies suggest that disclosure accuracy is an entrenched norm in SNS contexts. If participants perceive that this context is

similar to other SNSs (e.g., Facebook), they may disclose more accurately in accordance with the entrenched norm when eye primes are present:

H5: Participants' disclosures will be more accurate when eye primes are present then when they are absent.

Privacy Setting Decisions

This study will also explore how disclosure frequency and accuracy may affect transmission principles that regulate who can see a user's disclosures: privacy setting decisions. Recall that transmission principles place constraints on the distribution and/or dissemination of sensitive information from party to party within a context, prescribing when the transfer of information is appropriate (Nissenbaum, 2010). Privacy settings can help users feel as though they are placing appropriate constraints on who can see/access the content they disclose online (Brandimarte, Acquisti, & Loewenstein, 2013). As a result, participants in this study may select stricter privacy settings after disclosing a larger proportion of information on their profiles. However, given that users tend to select open privacy settings when they first join a SNS so that other users can find them on the site (Joinson, 2008), participants in this study may select more open settings to help them build their network in this context.

How accuracy will affect privacy setting decisions is similarly unclear. Recent research has found that participants tend to omit, rather than inaccurately disclose, information in order to protect their privacy on Facebook (Chen & Marcus, 2012). This coupled with entrenched SNS norms that influence the likelihood that users will disclose often and accurately may mean that users will select open privacy settings after disclosing accurate information on their profiles. However, given that this study will ask for sensitive information that is typically perceived as inappropriate for the context, users may 1) select stricter settings if they have accurately disclosed inappropriate information, or 2) select open settings if they have inaccurately disclosed

inappropriate information. Given these possibilities, this study will examine how disclosure frequency and accuracy are related to privacy setting decisions:

RQ2: How does disclosure frequency and accuracy affect privacy setting decisions in this context?

Individual Differences in Disclosure Frequency & Accuracy Behavior

While the primary focus has so far been on how contextual cues and eye primes influence disclosure frequency and accuracy on SNSs, two key individual differences may influence users' adherence to contextual cues and/or entrenched norms in this context: self-monitoring and digital privacy literacy. Self-monitoring is a unique personality trait that can help explain why some people may be more or less likely to follow informational norms on a SNS Self-monitoring theory focuses on the extent to which an individual monitors and adjusts their behavior in order to fit in with context-relevant norms (Lennox & Wolfe, 1984). High self-monitors are characterized as closely monitoring and comparing their behavior to others' behavior. They strive to follow social norms and exhibit socially desirable behavior in order to project a positive impression and obtain social rewards. Low self-monitors are characterized as caring less for whether their behavior accommodates a social situation and tend to not monitor or compare their behavior to others' behavior as a result. Given that high-self monitors are especially concerned with adhering to norms, SNS users who are also high self-monitors may be more inclined to follow the norms indicated by the contextual cues in this context:

H6: High self-monitors are more likely to follow contextual cues than low self-monitors.

In addition to self-monitoring, digital privacy literacy is another individual difference that may affect whether or not a user follows contextual cues on a SNS. Digital privacy literacy is the extent to which an individual is knowledgeable about online information sharing practices. Park (2011) contends that failing to have insight into how data flows in novel digital contexts

hinders the complex decision-making process in disclosing information online. Therefore, those who are more informed about an online context's (e.g., a SNS) information sharing policies should be better able to discern what kinds of information are appropriate to disclose on a site, and should also be disinclined from following contextual cues that indicate a frequent disclosure norm in this context:

H7: Participants with higher levels of digital privacy literacy are less likely to follow contextual cues that indicate a frequent disclosure norm.

Direct versus Indirect Effect of Eyes on Behavior

While the research on eye primes suggests that they increase normative behavior, the extent to which this is a direct or indirect effect remains unclear. As discussed above, several studies examining eye prime effects confound contextual cues with indicated norms. This not only equivocates whether eye primes influence behaviors that are consistent with contextual cues or entrenched norms; it also equivocates whether eye primes were having direct or indirect effects on behavior. Social psychology scholars have long debated about whether primes have direct or indirect effects on behavior (Bargh, 2006; Bargh, Chen, & Burrows, 1996; Cesario, Plaks, Hagiwara, Navarette, and Higgins, 2010; Dijksterhuis & Bargh, 2001; Ferguson & Bargh, 2004; Loersch & Payne, 2011; Wheeler, Smeesters, & Kay, 2011). Direct effect advocates posit that contextual characteristics such as aspects of one's location (e.g., temperature, objects, and images) and/or aspects of an actor (race, age, etc.) activate in memory semantically related information that directly produces behavioral effects (Ferguson and Bargh, 2004). For example, being primed about an actor's age (e.g., that they are elderly) activates in memory stereotypical information about that actor's social category (e.g., they are hard of hearing), and may directly influence behavior (e.g., they automatically speak louder in response to the activated stereotype) (Bargh, Chen, & Burrows, 1996).

Indirect effect advocates take a different approach; they posit that primes first influence our perceptions of other actors, situations or locations, and/or the interaction itself, which then influences behavior according to the affective valence of the perception(s) (Smeesters, Wheeler, & Kay, 2010). For example, being primed about a person's age (e.g., that they are elderly) activates stereotypical information about that category (e.g., they are hard of hearing), but will only influence a speaker's volume if the speaker desires to interact with, or be heard by, an elderly person. That is, the speaker must be motivated to want to interact with elderly people in order for an elderly prime to indirectly affect their speaking volume.

Given these competing arguments, this study will test if eye primes indirectly increase normative behaviors or if they directly increase attentional focus. If eye primes directly increase attentional focus, participants should be able to recall more details about the site's design and features after they've exited the site. For example, participants should be more likely to recall aspects of the site's banner (e.g., that the banner contains the university's logo) when eye primes are present than when eye primes are not present on the site. However, if eye primes indirectly increase normative behavior, than in addition to increasing adherence to contextual cues, participants should be able to recall more about the behavioral trends conveyed in the contextual cues (e.g., most or few users have disclosed information on their profiles) when eye primes are present than when they are absent from the profile page. This study will test for whether eye primes directly increase attentional focus or indirectly increase normative behaviors by asking participants to list details about the site and trends conveyed in the contextual cues:

H8: If eye primes directly affect attentional focus, participants will recall more site details in the eye prime condition relative to the control image condition.

H9: If eye primes indirectly increase normative behavior, participants will recall more behavioral trends in the eye prime condition relative to the control image condition.

Methods

Participants

Participants were recruited via Cornell's SONA research participation websites, paper flyers, and quarter cards. Recruitment lasted from March 20th, 2014 to April 30th, 2014. One hundred forty-four participants completed the survey. There was one participant who entered jocular information in their profile (listed their hometown as "Tatooine", their major as "Jedi Knight", etc.); their data was removed. In addition, 13 participants mentioned the eye primes in their survey and their data was also removed. Participants' ages ranged from 19 to 26, with an average age of 21.25. Women were overrepresented in the data (68.9%), and participants mostly identified as either White (46.7%) or Asian (29.5%).

The "Cornell Campus Connect" SNS

The SNS used in this study was designed specifically to test how feedback and eye primes affect disclosure frequency and accuracy. The SNS, dubbed "Cornell Campus Connect" included a home page (Appendix B) that featured mock updates, images taken from the websites of each of the university's campuses, and a banner containing the university's and Social Media Lab's logos. The profile and privacy settings page was simpler in appearance than the home page; neither of them contained any user pictures or University images. Instead, the profile page contained profile information fields (shown in random order) and the privacy settings page contained the different settings. In Study 2, participants always saw the home page first, followed by the profile page, and then the privacy settings page.

Given that some of the fields asked for sensitive information (e.g., social security number), several measures were taken to ensure participant confidentiality. Only the following information was recorded: hometown, major, graduation year, relationship status, academic

accomplishments and college affiliation. After participant disclosures were checked, the recorded pieces of information were coded as either being filled out or left blank, and participants' actual disclosures were destroyed along with the PHP session at the end of the post study survey. All of the other disclosures (e.g., phone number, academic major) were automatically coded as having been entered (1) or left blank (0) in the dataset. In addition, to ensure that participants did not disclose bogus information, the profile fields that ask for numerical information (e.g., social security number, university ID number) required participants to disclose the appropriate amount of numbers or they were given an error message telling them they needed to fix their information or leave that field blank. As a result of these measures, this study was able to investigate what affects disclosure behavior on a SNS profile without infringing upon participant confidentiality as well as provide some confidence that participants' disclosures were genuine.

Procedure

Cornell Undergraduate students were recruited to participate in a "usability test" for the new SNS "Cornell Campus Connect". They were told that the site was intended to help students learn about academic and professional opportunities, and help them connect with other students, at Cornell's Ithaca and New York City Tech campuses. Recruitment materials informed participants where they could access the study online. The study began with a consent page, followed by the Cornell Campus Connect home page. After reviewing the home page, participants were directed to the profile page where they were asked to disclose inappropriate, somewhat appropriate, and appropriate information types. After filling out a profile, participants were asked to select one of four settings for who would be able to see the information they entered on their profile: 1) "Everyone", 2) "Cornell students, faculty, alumni, and staff", 3) "Cornell students only", or 4) "Only me", for 5 different privacy settings (Appendix E). After

selecting their privacy settings, participants were directed to the study's post-study survey (Appendix G).

The post-study survey explored certain situational and individual characters that were predicted to affect disclosure behavior. First, participants were asked to share their thoughts about the site (i.e., what can be improved). Then, participants were asked recognition questions that would determine if the eye primes had direct effects on attention versus indirect effects on normative behavior. Then they answered self-monitoring, Facebook self-monitoring, and digital privacy survey items. Then they were asked to rate the accuracy of their profile disclosures. Then they answered some demographic questions, followed by a few debriefing questions. Finally, they were thanked for their time and given instructions about how to receive their compensation.

Appropriateness. The data from Study 1, which revealed what kinds of information university students perceive as too sensitive and therefore inappropriate to share on a profile for a university affiliated SNS, provided the basis for the profile information fields in Study 2. For example, participants from Study 1 perceived sensitive information such as their social security number as inappropriate, but less sensitive information such as graduation year as appropriate to share on a university affiliated SNS profile. The profile page asked for 18 pieces of information; 5 pieces of information came from the inappropriate information category, 8 pieces of information came from the somewhat appropriate information category, and 5 pieces of information came from the appropriate information category. The final list of information that was included on the profile page is presented in Table 3. In addition, some of the language for the profile fields was adapted to make it easier for participants to disclose parsimonious responses. For example, the information label "relationship history" in Study 1 was changed to

"number of past romantic relationships" in Study 2, so that participants would have an easier time disclosing their information into this field.

Contextual Cues. The norms indicated by the contextual cues were presented via histograms that demonstrated how many users had disclosed different kinds of information on their profiles (Appendix C). The high cues condition featured histograms that indicated most users had disclosed their information on their profiles (e.g., a histogram that depicts 71% of users disclosed their graduation year onto their profile versus 29% leaving the graduation year information field blank). In contrast, the low cues condition featured histograms that indicated few users had disclosed their information on their profiles (e.g., a histogram that depicts 39% of users disclosed their graduation year onto their profile versus 61% leaving the graduation year information field blank). There was also a no cues condition that did not display any histograms on the profile page.

While this procedure draws on Acquisti et al.'s (2012) methodology, there is an important difference between their study and this study's presentation of contextual cues. Acquisti et al. (2012) showed participants contextual cues only after they had or had not answered a question; the current study presents the contextual cues on the site before participants have filled out their profile. This is because the primary goal is to understand how contextual cues can affect how SNS users disclose individual pieces of information that range in appropriateness whereas Acquisti et al. (2012) was interested in whether they could increase the overall response rate.

Eyes Primes. The eye primes or control image was embedded in the Social Media Lab logo located on the right hand side of the banner at the top of the profile page (Appendix D). The banner was fixed so that even when participants scroll down the profile page, the banner and

prime/image was still visible. The eye prime or control image in the banner was also present during the privacy setting decision phase.

Dependent Measures. Entrenched norms were measured by calculating how often and how accurately participants disclosed information on their profiles. Participants' disclosure rate was calculated by computing on average how frequently participants disclosed overall, and how frequently they disclosed inappropriate, somewhat, and appropriate information types respectively (see Table 4). Disclosure accuracy was calculated by computing on average how accurately participants rated their disclosures overall and how accurately they rated their inappropriate, somewhat appropriate, and appropriate disclosures in the post-study survey (see Table 4). Privacy settings was calculated by tallying how often participants selected open versus strict privacy settings (Cronbach's $\alpha = 0.87$, $GM = 2.34$, $SD = 0.75$), and were averaged to yield a single privacy setting factor.

Individual Difference Measures. The individual difference variables were assessed using validated scales. To assess self-monitoring, participants were asked questions adapted from Lennox and Wolfe's (1984) self-monitoring scale as well as an adapted version examining self-monitoring behavior as it relates to the SNS Facebook (Litt et al., 2014) (See Appendix F). For example, participants indicated agreement with items such as "I have the ability to control the way I come across to people depending on the impression I wish to give them" on a scale of 1 (strongly disagree) to 5 (strongly agree). The items for the self-monitoring scale (Cronbach's $\alpha = 0.81$, $M = 3.75$, $SD = 0.46$) and the items for the Facebook self-monitoring scale (Cronbach's $\alpha = 0.81$, $M = 3.74$, $SD = 0.58$) were averaged into two separate factors. Self-monitoring and Facebook self-monitoring were also dichotomized by placing participants in the bottom quartile into the "low" category and placing participants from the top quartile (4.08) into the "high"

category. For self-monitoring, there were 30 participants in the bottom quartile (3.49) and 27 participants in the top quartile (4.08). For Facebook self-monitoring there were 32 participants in bottom quartile (3.29) and 31 participants in the top quartile (4.14).

Participants were then asked about their individual levels of digital privacy literacy. The digital privacy literacy scale is composed of three sections, examining a user's familiarity with online technology, awareness of online surveillance practices, and understanding of general online policies (Park, 2011) (See Appendix F). The technical familiarity subsection of the scale contained 10 items that ask participants to rate how familiar they are with 10 different technologies (e.g., PHP) on a 6-point scale (1= not at all familiar, 6 = very familiar) (Park, 2011). The items examining technical familiarity were reliable (Cronbach's $\alpha = 0.86$, $M = 3.35$, $SD = 0.99$). The surveillance practice subsection contained 8 true/false items. Participants' correct answers were summed into a single surveillance practices factor ($M = 6.46$, $SD = 1.40$). The policy understanding subsection of the scale contained 7 true/false items. Participants' correct answers were summed into a single policy understanding factor ($M = 3.84$, $SD = 1.62$). Technical familiarity, surveillance practices, and policy understanding were also dichotomized by placing participants from the bottom quartile into the "low" category and placing participants from the top quartile into the "high" category. For technical familiarity, there were 31 participants in the bottom quartile (2.50) and 25 participants in the top quartile (4.13). For surveillance practices, there were 26 participants in the bottom quartile (2.60) and 27 participants in the top quartile (4.00). For policy understanding there were 57 participants in the bottom quartile (3.00) and 41 participants in the top quartile (5.00).

Eyes Mechanism Measures. To examine the direct versus indirect effects of the eye primes, participants were asked recognition questions, pertaining to site details and user norms

that would determine if the eye primes had direct effects on attention versus indirect effects on normative behavior. Participants' answers to the detail, low norm, and high norm questions were summed into three separate factors.

Results

This study employed a 3 (inappropriate, somewhat appropriate, appropriate information type) X 3 (high, low, or no) X 2 (eye prime or control image) between-subjects design to investigate how information appropriateness, contextual cues, and eye primes affect disclosure and accuracy behavior on a SNS profile.

The following analyses used a linear mixed model in SPSS v19 where the disclosure behavior (i.e., frequency or accuracy) was entered as the dependent variable, information appropriateness level (inappropriate, somewhat appropriate, and appropriate), contextual cue (no, low, and high), and eye primes (eye image versus control), were entered as independent variables.

Disclosure Frequency

The first set of analyses focus on how frequently participants disclosed information in this context.

Appropriateness. Consistent with H1, participants differentially disclosed information according to its appropriateness level $F(2, 348) = 169.15 = p < 0.001$. As predicted, participants disclosed information that was evaluated as inappropriate for this context least frequently, followed by somewhat appropriate information, and disclosed information that was appropriate for this context most frequently (see Table 4). This is consistent with Nissenbaum's (2010) contention that people differentially disclose information depending on whether they think it is appropriate for the context.

Contextual Cues. H2 predicted that contextual cues would affect how frequently participants disclosed in this context. Consistent with H2, contextual cues significantly affected the likelihood a participant would disclose information regardless of appropriateness level, $F(2, 348) = 20.67$, $p < 0.001$ (see Figure 1). Pairwise comparisons revealed that participants disclosed less frequently in the low compared to the high cues condition ($p < 0.001$), and disclosed less frequently in the low compared to the no cues condition ($p < 0.001$). However, in contrast to H2, participants disclosed *less* frequently in the high compared to the no cues condition ($p < 0.05$).

Eyes. H3A predicted that eye primes would increase the likelihood that participants would follow the contextual cues in this context. The predicted interaction between eye primes and contextual cues was marginally significant, $F(2, 348) = 2.86$, $p < 0.06$. In contrast to H3A, however, the eye primes increased disclosure rates in both the low $F(1,123) = 4.24$, $p = 0.05$, and in the high $F(1, 102) = 3.85$, $p < 0.05$, cues conditions, but not in the no cues condition [$F(1,123) = 0.73$, $p = 0.40$] (see Figure 1). This pattern does not support H3A, which predicted that the eye primes would decrease disclosures in response to the low disclosure cue but increase disclosures in response to the high disclosure cue.

Instead, the pattern of responses was consistent with H3B, which predicted that eye primes would increase adherence to the entrenched norm. Given that both low and high contextual cues decreased disclosure rates relative to the entrenched norm, to support H3B the eye primes should increase disclosure rates. The main effect of eye primes revealed this to be the case, $F(1,348) = 3.99$, $p < 0.05$, with participants disclosing more when the eye primes were present ($M = 53.8\%$, $SE = 0.02$) than when they were not present ($M = 48.6$, $SE = 0.02$) (see Figure 1). These results suggest that eye primes increase disclosure frequency in accordance with the entrenched norm in this context.

Accuracy

The following set of analyses focus on how accurately participants disclosed information in this context.

Appropriateness. H4 predicted that participants would disclose inappropriate information less accurately than appropriate information. Consistent with H4, participants disclosed information that was inappropriate for this context least accurately, followed by somewhat appropriate information, and disclosed information that was appropriate for this context most accurately, $F(2, 348) = 169.15 = p < 0.001$ (see Figure 2).

Eyes. H5 predicted that the eye primes increase participants' adherence to the accurate disclosure norm observed in other SNS contexts. Partially consistent with H5, participants' disclosures were marginally more accurate when eyes were present rather than absent from the profile page $F(2,338) = 3.55$, $p = 0.06$. There was, however, an unexpected interaction between eye primes and contextual cues, $F(2,338) = 5.55$, $p < 0.01$. As depicted in Figure 2, when looking exclusively at the low cues condition, participants' disclosures were more accurate when eyes were present than when they were absent $F(1,115) = 10.84$, $p < 0.01$. However, eyes did not affect the accuracy of participants' disclosures in the no cue [$F(1,121) = 0.84$, $p = 0.36$] or high cue condition [$F(1,102) = 1.38$, $p = 0.71$].

Privacy Settings

RQ2 asked if disclosure frequency would affect participants' privacy setting decisions. A correlation between privacy settings and disclosure frequency revealed that the more frequently a participant disclosed information on their profile, the more open they set their privacy settings $r(122) = 0.24$, $p < 0.01$. However, this effect was only found for appropriate $r(122) = 0.22$, $p < 0.05$, and somewhat appropriate $r(122) = 0.26$, $p < 0.01$ information, but not for inappropriate

information [$r(122) = 0.12$, $p = 0.21$]. This suggests that participants were mindful that their disclosures would be considered appropriate by a potentially large and diverse audience.

RQ2 also asked if disclosure accuracy affects participants' privacy setting decisions. There was a positive relationship between accuracy and privacy setting decisions $r(122) = 0.27$, $p < 0.01$. Moreover, this effect was found for appropriate $r(122) = 0.29$, $p < 0.01$, somewhat appropriate $r(120) = 0.30$, $p < 0.01$, and inappropriate information $r(114) = 0.21$, $p < 0.05$. However, given that participants disclosed inappropriate information less frequently, these results suggest that users likely resort to omitting rather than inaccurately reporting their inappropriate information in order to ensure their privacy and uphold relevant transmission principles in this context.

Individual Differences

The following set of analyses focus on how the individual difference variables affect disclosure behavior.

H6 predicted that high self-monitors would be more likely to follow contextual cues than low self-monitors. To test this hypothesis, disclosure rate was entered as the dependent variable, and contextual cues and the dichotomized self-monitoring factors were entered as independent variables, into a linear mixed model. In contrast to H6, neither self-monitoring [$F(2,99) = 0.27$, $p = 0.76$], nor Facebook self-monitoring [$F(2,99) = 0.53$, $p = 0.59$], influenced the likelihood a participant would disclose according to the contextual cues.

H7 predicted that participants with higher levels of digital privacy literacy would be less likely to follow contextual cues when they depict most users have disclosed inappropriate information on their profiles. To test this hypothesis, disclosure rate was entered as the dependent variable, and contextual cues and the digital privacy literacy factors were entered as

independent variables, into a linear mixed model. In contrast to H7, none of the digital privacy literacy factors affected whether participants followed the contextual cues (technical familiarity [F(2,78) = 0.72, p = 0.49], surveillance practices [$F(2,78) = 0.10$, $p = 0.91$], policy understanding [$F(2,132) = 2.14$, $p = 0.12$]).

Eyes Mechanism

The next set of hypotheses explores the extent to which eye primes have direct or indirect effects on behavior.

H8 predicted that if eye primes have a direct effect on attention, participants should be able to answer more of the detail questions about the Cornell Campus Connect site when eye primes are present than when they are absent from the profile page. In contrast to H8, the eye primes did not affect whether participants answered the detail questions correctly (see Table 5). H9 predicted that if eye primes have an indirect effect on the salience of norms, participants should be able to answer more of the norm questions pertaining to the contextual cues when eye primes are present than when eye primes are absent from the profile page. In contrast to H9, the eye primes did not affect whether participants answered the norm questions correctly in the low or high cues conditions (See Table 5).

Discussion

The goal of Study 2 was to examine how contextual cues and eye primes affect disclosure behavior in a SNS context. Recent research has found that users disclose frequently and accurately across various SNSs (Chen & Markus, 2012; Hancock & Toma; Lampe et al., 2007; Madden et al., 2013), suggesting these disclosure behaviors are entrenched as normative in SNS contexts. Participants applied these entrenched norms to the Cornell Connect SNS, disclosing with high frequency and accuracy. Moreover, they also disclosed appropriate information more

frequently than inappropriate information, suggesting they were disclosing in this context as they would on other SNSs. The contextual cues indicating how others had disclosed on the site affected participants' disclosure behavior, though not always as expected. When the cues indicated a low disclosure frequency norm, participants disclosed less frequently relative to where there were no cues present. However, when the cues indicated a high disclosure frequency norm, participants also disclosed less frequently relative to when there were no cues present. The presence of eye primes increased disclosure frequency and accuracy relative to when they were not present, primarily when the contextual cues suggested participants should deviate from the entrenched norm, suggesting that the eye primes promote adherence to entrenched norms. These findings have important implications for Nissenbaum's (2010) framework of contextual integrity and our understanding of how eye primes influence behavior.

Implications for the Framework of Contextual Integrity

Nissenbaum's (2010) framework of contextual integrity posits that privacy is determined by informational norms that prescribe when it is appropriate to disclose information with sensitive attributes in a given context. Informational norms are characterized by key cues such as contextual similarity (i.e., whether the present context is similar to previously encountered contexts) and information attributes (i.e., how sensitive a piece of information is perceived to be). For example, in Study 1, information that was perceived as having sensitive was also evaluated as inappropriate to disclose in a university affiliated SNS. The data from Study 2 provide additional evidence for this proposition; participants disclosed information perceived as sensitive less frequently than information perceived as appropriate for this context. This suggests that participants' disclosure intentions from Study 1 were replicated in participants' actual disclosure behavior in Study 2. Moreover, these results highlight how information attributes

such as sensitivity influence users' willingness to disclose different kinds of information in this context.

Sensitivity as an Informational Attribute. Consistent with Nissenbaum (2010), participants in Study 2 used information attributes to determine whether they should disclose a piece of information in a context. More specifically, participants disclosed information with sensitive attributes (e.g., social security number) less frequently, suggesting they perceive information with sensitive attributes as inappropriate to disclose in this context. Participants also disclosed sensitive or rather information that is inappropriate for this context less accurately. While previous work has found that users sometimes inaccurately disclose information on a SNS profile in order to appear more attractive (Toma et al., 2008), the present work suggests that users may inaccurately disclose information because they perceive it as inappropriate (i.e., too sensitive) for the context. Perhaps participants resorted to inaccurately disclosing information so they could appear open while simultaneously protecting their privacy. This suggests that, in addition to omitting information, SNS users may also inaccurately disclose information in order to preserve their privacy.

When a Cue is a Clue. Given that most SNSs obscure key cues that determine the appropriateness of a disclosure in offline contexts, Study 2 examined if cues indicating disclosure norms would affect disclosure behavior in a SNS context. To test this, participants were presented with cues containing histograms that indicated different levels of disclosure rates. The "low cues" contained histograms indicating few users disclosed information on their profiles, and the "high cues" contained histograms indicating most users disclosed information on their profiles. In other words, the low and high cues provided normative information by indicating how frequently other users had or had not disclosed information that varies in

appropriateness on their profiles. Participants disclosed less frequently when there were low rather than no cues on the profile page, suggesting that participants interpreted the low cues as disclosure prescriptions indicating they *should not* disclose a lot of information in this context. Moreover, post hoc analyses revealed that the low cues decreased disclosure rates for each type of information, including inappropriate, somewhat appropriate, and appropriate information, suggesting that the low disclosure cue potentially led participants to perceive that relevant information (e.g., academic major) was inappropriate because other users had refrained from disclosing that information in this context. This is consistent with Nissenbaum's (2010) contention that contextual cues can affect disclosure behavior, as well as the perceived appropriateness of a disclosure, in a SNS context.

When A Cue is Not a Clue. The high disclosure cues, which indicated that most users had disclosed a lot of information on their profile, were not only ineffective at increasing participants' disclosure rates, they actually decreased how much participants disclosed in this context relative to the entrenched norm. This raises the possibility that both the high and low disclosure cues merely reminded participants that users vary how much they disclose on their SNS profiles, potentially implying that the participants themselves do not have to disclose all of their information in this context. This does not seem to be the case as participants disclosed less frequently in the low disclosure cue condition relative to the high disclosure cue condition, suggesting that participants were indeed interpreting these cues differently.

Nonetheless, why did the high disclosure frequency cue constrain disclosure behavior? One possibility is that the high cues may have aroused suspicion that they were not indicating disclosure norms but were actually a ploy to get them to disclose more information on their profiles. For example, it is probably not plausible that participants trusted cues that indicated

68% of users had disclosed their social security number in this context because of expectations that few people would likely disclose such private information on a SNS. Instead, participants likely perceived this cue as ploy intended to get them to disclose information they know is inappropriate for this context. If this were the case, it suggests that contextual cues may influence whether or not users engage in behaviors that violate entrenched norms, but that there are limits on how different those contextual cues may be from expected social norms.

It is also possible that the "high" cue just wasn't "high" enough. For example, when there were no cues or eyes primes on the profile page, participants disclosed appropriate information types 88.7% of the time. The high cues indicated that other users had disclosed appropriate information types approximately 70% of the time. This suggests that the high cue was in fact not high enough to influence participants' willingness to disclose more than they would without the cues. Future research should adjust cues that indicate different levels of disclosure rates so that they better reflect how participants disclose different kinds of information in a SNS context.

Eye Primes: Effects and Mechanisms

Eye Primes Influence Entrenched Norms. Study 2 attempted to uncover how eye primes affect normative behavior: do they increase behaviors that are consistent with norms entrenched in a context or norms that are indicated by contextual cues? Previous studies have failed to differentiate between entrenched and indicated norms. For example, Bateson and colleagues (2006) placed eye primes on a sign that contained cues prescribing patrons to pay for their milk, expecting the primes would affect the likelihood that patrons would pay for their milk. However, it was expected that patrons would pay for their milk long before these interventions were embedded in their break room. As a result, there was no way of deciphering whether eye primes were influencing behaviors that were already entrenched as normative in this

context or if they were influencing behaviors that were normative as indicated by a contextual cue.

This study sought to distinguish between adherences to the entrenched norm from adherence to the indicated norm. For example, while SNSs are entrenched with norms that prescribe users to disclose frequently and accurately, as evidenced by prior work (Chen & Markus, 2012; Hancock & Toma; Lampe et al., 2007; Madden et al., 2013) and the results from the present study, the contextual cues contained normative information that were either consistent (high disclosure cues) or inconsistent (low disclosure cues) with the entrenched norm. By differentiating the entrenched norm from the contextual cues, Study 2 can determine if eye primes increase behaviors that are consistent with entrenched or indicated norms. If eye primes increase adherence to indicated norms, we would expect the eye primes to enhance the effect of the contextual cue. In contrast, the results revealed that the eye primes increased how frequently and accurately participants disclosed when there were low disclosure cues (i.e., cues that contrasted the entrenched norm) on the profile page, suggesting that eye primes increase behaviors that are entrenched as normative in a context, and should increase behaviors that people ought to do. For example, in SNSs users feel they should disclose frequently and accurately, and the eye primes increased these disclosure behaviors when other cues discouraged these behaviors. Similarly, when eye primes were featured in dictator games, they seemed to push participants to allocate roughly half of their winnings with another player because they felt they ought to give a fair rather than a stingy or exceedingly generous amount (Nettle et al., 2013).

What Drives Eye Prime Effects? This study also attempted to uncover what drives eye prime effects by examining if they directly or indirectly increase normative behavior. To test

this, participants answered questions that pertained to the details and norms on the site. It was expected that if eye primes directly affect attentional focus, participants should have been able to correctly answer detail questions more often when eye primes were present than when they were not present. Similarly, if eye primes indirectly increase normative behavior, participants should have been able to correctly answer questions about the norms contained in the cues more often when eye primes were present than when they were not present. Unfortunately, the eye primes did not affect participants' ability to correctly answer the detail and/or norm oriented questions, suggesting that the data were inconclusive regarding whether eye primes directly affected attention or indirectly affected normative behavior.

Individual Differences

The self-monitoring and digital privacy literacy factors did not have any effect on the likelihood that participants would disclose in accordance with the contextual cues. In addition, none of these factors were related to disclosure accuracy. It is possible that these individual difference variables affect SNS behavior, but perhaps not disclosure frequency and accuracy specifically.

Overall, contextual cues and eye primes affected how frequently and how accurately participants disclosed information on their profiles. In addition, the relationships between disclosure behavior and privacy settings suggest that participants wanted a larger proportion of other users to be able to see their profiles so long as their disclosures were appropriate for the context. Considering that privacy setting decisions are another kind of SNS behavior that is affected by norms, this study will also explore how contextual cues and eye primes influence privacy setting decisions.

Study 3 – Contextual Cues, Primes and Privacy Settings

Nissenbaum's (2010) framework of contextual integrity, which posits that people use contextual cues to help them abide by a context's informational norms, can also be applied to users' privacy setting decisions. Transmission principles, one of the four key cues outlined in Nissenbaum's (2010) framework, place constraints on the distribution and/or dissemination of information from party to party within a context, prescribing when the transfer of information is appropriate. Privacy settings are meant to help users abide by relevant transmission principles by regulating who can access a piece of information or disclosure in a SNS context. For example, users who disclose sensitive information (i.e., health issues) on their profile may select a stricter privacy setting to conceal their disclosure from certain actors (e.g., their professors) to ensure the appropriateness of their disclosure. That is, selecting strict privacy settings is a means of addressing transmission principles in the SNS context.

Stricter settings, however, do not necessarily ensure that inappropriate actors will be restricted from seeing a sensitive disclosure (Brandimarte et al., 2013; Liu et al., 2011). This is because strict privacy settings do not bar members from a user's network from sharing their disclosures with other unauthorized users (Acquisti & Gross, 2006), nor do they restrict site owners from selling their disclosures with unauthorized third parties (e.g., advertisers) (Fuchs, 2012). The SNS context therefore makes it difficult for users to determine if the privacy settings they are selecting will help them uphold a SNS's informational norms. Under these circumstances, how do people make decisions around privacy settings on SNSs?

This study proposes that contextual cues and eye primes may be able to affect privacy setting decisions in a SNS context. In addition, most SNSs require users to fill out a profile before selecting privacy settings. This order of behaviors may increase how much users disclose and how open they set their privacy settings. This raises the question whether placing the privacy

settings before the profile page might affect participants' disclosure behavior on the site. Can placing the privacy setting page before the profile page heightens users' perception of control over their information, which in turn may influence how much and how accurately they disclose information in a SNS context? The third study in this dissertation addresses these questions by examining how contextual cues and eye primes affect decisions about privacy settings, and how these decisions affect subsequent disclosure behavior.

Privacy Settings, Entrenched Norms and Contextual Cues

Past research on SNS privacy setting choices has found that users tend to select open privacy settings (e.g., making one's profile open to the public), suggesting that selecting open privacy settings is the entrenched norm in a new SNS context. Users typically engage with SNSs to connect with and build networks comprising of people they already know offline (Ellison et al., 2007; 2011). Selecting open privacy settings helps other users search for and find a user's profile on a SNS. This is exactly what earlier studies examining user privacy setting decisions found; users typically selected open settings when they joined a SNS (Acquisti & Gross, 2006; Barnes, 2006; Ellison et al., 2007; Govani & Pashley, 2005; Gross & Acquisti, 2005; Jones & Soltren, 2005) because they wanted to make new connections and build a large network on these sites (Joinson, 2008). These consistent patterns of results suggest that users expect each other to select open settings because it helps them find each other on SNSs (Lampe et al., 2007). The context used in this study, which is the same as that described and used in Study 2, was designed to feel similar to early iterations of Facebook (e.g., only members of a university community could join, etc.) (boyd & Ellison, 2007). As a result, participants are expected to select open settings more frequently than strict settings in this context.

Although open privacy settings help users connect with others and build their network on a SNS, they can undermine transmission principles resulting in minor to serious privacy violations (Litt et al, 2014). When users select open privacy settings, they allow a wide range of others to access their disclosures on a SNS. Users tend to assume that close others (e.g., their friends and classmates) will look for their profile more than non-close others (e.g., their professors) (Ellison et al., 2007). As a result, open privacy settings may make users vulnerable to transmission principle violations. For example, offline transmission principles proscribe a student from disclosing about his problems with insomnia to his T.A. because the T.A. cannot be trusted to withhold his sensitive insomnia disclosure from his professor. However, let's imagine this student wants to find other students who also suffer from insomnia at his university, and proceeds to disclose about his insomnia on his SNS profile. Although he expects that only his friends and classmates will see his sensitive disclosure, his open settings allow his T.A. to also see his sensitive disclosure. The T.A. can proceed to disclose about the student's insomnia issues with his professor, not only resulting in the violation of transmission principles but also potentially jeopardizing the professor's opinion of the student.

Given that the entrenched norm is to select open settings when initially joining a new SNS (Acquisti & Gross, 2006; Barnes, 2006; Ellison et al., 2007; Govani & Pashley, 2005; Gross & Acquisti, 2005; Jones & Soltren, 2005), but selecting open settings can result in transmission principle violations, what kinds of cues can help them select privacy settings that will ensure their own and other users' privacy? One potential cue is other users' privacy setting decisions. US Facebook users were found to have strict privacy settings when their friends and especially their roommates had also selected strict privacy settings (Lewis, Kaufman, & Christakis, 2008; Utz & Krämer, 2009). Similarly, users of the Dutch SNS Hyves were more likely to have

selected strict privacy settings if they perceived their friends had also selected strict privacy settings (Utz & Krämer, 2009, Studies 2 & 3). Utz and Krämer (2009) posit that one of the ways users glean privacy setting norms is by keeping tabs on whose profiles they can and cannot access in their network. If users model their privacy setting decisions after other users' privacy setting decisions, contextual cues that indicate how others are making privacy setting decisions should influence how users set their privacy settings.

While Nissenbaum's (2010) framework of contextual integrity focuses on how contextual cues affect disclosure behavior, contextual cues should also be able to affect privacy setting behavior, given that both types of behaviors influence a user's ability to uphold transmission principles on SNSs. For example, the contextual cues in Study 2 that indicated few users disclosed information on their profiles decreased how frequently participants' disclosed information in this context. If instead contextual cues indicate that most users select strict privacy settings, then newer users should select stricter settings so that their behavior matches the norm indicated by the cue. Similarly, if contextual cues indicate that most users select open privacy settings, newer users should follow the cue and select more open privacy settings. Based on this rationale and the findings from Study 2, the following hypothesis was derived for Study 3:

H1: Participants will select stricter settings when strict privacy setting contextual cues are present and select more open privacy settings when open privacy setting contextual cues are present relative to when no contextual cues are present.

Eye Primes and Privacy Setting Decisions

Several social psychology studies, as well as the result from Study 2, suggest that eye primes increase behaviors that are consistent with norms that are entrenched in a given context. For example, eye primes increased how often participants' picked up their litter in a cafeteria

context even where there were no contextual cues prescribing they should do so (Ernest-Jones et al., 2011). Study 2 found that users disclosed more frequently when there were contextual cues that prescribed them to disclose less frequently, suggesting that eye primes may be especially effective at influencing whether or not people follow entrenched norms in a given context. Given that users believe they should select open settings when they begin using a SNS (Ellison et al., 2007; Lampe et al., 2007), eye primes should influence whether or not participants select open settings when there are contextual cues that prescribe strict privacy setting behavior.

H2: Participants select more open privacy settings when eye primes are present than when they are not present in the strict cue condition.

Effects of Privacy Settings on Disclosure Behavior

If users are likely to select open privacy settings after first disclosing information in their profile according to entrenched norms on SNSs (Study 2), will they follow those same norms if they are required to select privacy settings before disclosing information in the profile (Study 3)? Most SNSs appear to be designed as if they were prompting users to disclose frequently and accurately on these sites (Christofides, Muise, & Desmarais, 2012; Nosko, Wood, & Molema, 2010; Rosen, 2010). As noted, users who spend time crafting a detailed yet accurate profile typically proceed to select open privacy settings so that they are more likely to meet their social goals on the site (Lampe et al, 2007.

In contrast, requiring users to select privacy settings first may highlight transmission principles rather than social goals. For example, when participants were led to perceive they had more control over who could access their disclosures on a SNS profile, they tended to disclose more sensitive information, a finding referred to as the privacy paradox (Barnes, 2006; Brandimarte et al., 2013). The privacy paradox suggests that the more control users feel they have over their information, the more likely they will disclose sensitive and therefore

inappropriate information on a SNS. This suggests that allowing users to set controls over their information via privacy setting should influence whether or not they disclose more inappropriate information on a SNS profile. Study 3 will examine how placing the privacy settings page before the profile page affects disclosure behavior relative to Study 2, in which participants disclosed information first and then selected privacy settings.

H3: Participants disclose more inappropriate information if they select privacy settings before they fill out a profile in this context.

However, the privacy paradox does not make any predictions about disclosure accuracy. It is possible that if users' perception of control over their information is enhanced by selecting settings prior to filling out a profile, participants may disclose information more accurately than if they had filled out a profile before selecting privacy settings. However, being asked to select privacy settings first may raise concerns about their privacy and lead participants to disclose less accurately in order to better protect their information. Given these opposing possibilities, Study 3 will explore:

RQ1: How is disclosure accuracy affected by asking participants to select privacy settings before filling out a profile?

Individual Differences in Privacy Setting Decisions

Although self-monitoring and digital privacy literacy did not affect disclosure frequency and accuracy in Study 2, it is possible that they may affect privacy setting decisions in Study 3 given that privacy setting decisions are influenced by norms and informed by wariness of online privacy issues.

Past research has found that users sometimes select privacy settings to match their friends' privacy settings (Lewis et al., 2008; Utz & Krämer, 2009). Given that high self-monitors

and high Facebook self-monitors are motivated to follow social norms, they may be more inclined to select privacy settings according to what is prescribed in the contextual cues:

H4: High self-monitors are more likely to select privacy settings that follow contextual cues than low self-monitors.

Users tend to believe that selecting stricter privacy settings can effectively control who can access their disclosures on these sites (Brandimarte et al., 2013). As a result, those who are especially digital privacy literate may be more inclined to select stricter settings so they can feel assured that their disclosures are protected:

H5: Participants with higher levels of digital privacy literacy are less likely to select open privacy settings.

Eyes Mechanisms

Although the measures examining whether eye primes have direct or indirect effects in Study 2 were inconclusive, they were included in Study 3 to capture how eye primes might be unconsciously affecting attention to detail and/or awareness of the norms contained in the contextual cues:

RQ2: Do eye primes affect participants' ability to recall details about the SNS and/or the indicated norms contained in the contextual cues?

Methods

Participants

Participants were recruited via Cornell's SONA research participation websites, paper flyers, and quarter cards. Recruitment lasted from May 2nd, 2014 to May 21st, 2014. One hundred and twelve participants completed the survey. There were 6 participants who mentioned the eye primes in their survey and their data was removed. Participants' ages ranged from 19 to 26, with an average age of 21.33. There were slightly more women (56%) than men, and participants mostly identified as either White (43.0%) or Asian (36.4%).

System

The SNS used in Study 3 was the same SNS used in Study 2 except for three key changes. First, the order of the profile information and privacy setting decisions was reversed relative to Study 2. In the present study, participants completed the privacy settings page first and then the profile page. Second, the contextual cues were featured on the privacy settings page rather than the profile page. Third, the contextual cues indicated privacy setting norms rather than disclosure frequency norms.

Procedure

The procedure for Study 3 was identical to Study 2, except participants were asked to select privacy settings before filling out a profile.

Contextual Cues. The strict cues condition featured histograms that indicated most users had selected strict privacy settings (e.g., 54% had selected "Only Me", 26% has selected "Cornell Students Only", etc.), whereas the open cues condition featured histograms that indicated most users had selected more open privacy settings (e.g., 54% had selected "Everyone", and 26% had selected "All Cornell", etc.). The no cues condition did not include any histograms. The contextual cues were presented in histograms similar to those used in Study 2 (Appendix F).

Eye Primes. The same eye prime and control images used in Study 2 were also used in Study 3.

Dependent Measures. Following the procedure for Study 2, privacy settings were calculated by tallying how often participants selected open versus strict privacy settings. Participants' decisions were reliable (Cronbach's $\alpha = 0.90$, $GM = 2.32$, $SD = 0.83$) and were averaged to yield a single privacy setting factor, from strict = 1 to open = 4.

Following Study 2, disclosure frequency was calculated by computing on average how frequently participants disclosed overall and how frequently they disclosed inappropriate, somewhat appropriate, and appropriate information types respectively (See Table 6). Disclosure accuracy was calculated by computing on average how accurately participants rated their disclosures overall, and how accurately they rated their inappropriate, somewhat appropriate, and appropriate disclosures in the post-study survey (see Table 6).

Individual Difference Measures. The individual difference variables were assessed using the same validated scales from Study 2. The items for the self-monitoring scale (Cronbach's $\alpha = 0.83$, $M = 3.62$, $SD = 0.49$) and the items for the Facebook self-monitoring scale (Cronbach's $\alpha = 0.74$, $M = 3.69$, $SD = 0.57$) were averaged into two separate factors. Self-monitoring and Facebook self-monitoring were also dichotomized by placing participants in the bottom quartile into the "low" category and placing participants from the top quartile into the "high" category. For self-monitoring, there were 20 participants in the bottom quartile (3.38) and 26 participants in the top quartile (3.92). For Facebook self-monitoring there were 26 participants in bottom quartile (3.71) and 35 participants in the top quartile (4.00). The items examining technical familiarity were reliable (Cronbach's $\alpha = 0.89$, $M = 3.40$, $SD = 1.10$) and were collapsed into a single factor. The correct answers to the surveillance practice items were summed into a single factor ($M = 6.85$, $SD = 1.13$), as were the correct answers to the policy understanding items ($M = 4.08$, $SD = 1.65$). Technical familiarity, surveillance practices, and policy understanding were also dichotomized by placing participants from the bottom quartile into the "low" category and placing participants from the top quartile into the "high" category. For technical familiarity, there were 26 participants in the bottom quartile (2.60) and 27 participants in the top quartile (4.00). For surveillance practices, there were 28 participants in the

bottom quartile (6.00), and 32 participants in the top quartile (8.00). For policy understanding there were 37 participants in the bottom quartile (3.00) and 41 participants in the top quartile.

To examine the direct versus indirect effects of the eye primes, participants were asked the same recognition questions that they were asked in Study 2. Participants' answers to the detail ($M = 3.98$, $SD = 1.27$), strict norm ($M = 2.55$, $SD = 1.66$), and open norm ($M = 1.81$, $SD = 1.26$) questions were summed into three separate eyes mechanism factors.

Results

This study employed a 3 (contextual cue: strict vs. open vs. no) X 2 (eye prime vs. control image) between-subjects design to investigate how contextual cues and eye primes affect privacy setting decisions. The study also examined disclosure frequency and accuracy across information appropriateness level (appropriate vs. somewhat appropriate vs. inappropriate) after participants had completed their privacy decisions.

Privacy Settings

Privacy setting decisions were analyzed with a linear mixed model in SPSS v19 where privacy settings was entered as the dependent variable, and contextual cue (strict, open, or no) and eye primes (eye image versus control) were entered as independent variables.

Consistent with H1, the data revealed that, contextual cues significantly affected how strict or open participants set their privacy settings in this context, $F(2, 98) = 3.11$, $p < 0.05$ (see Figure 3). The data fit the expected pattern; participants selected stricter settings in the strict relative to the open cues condition. Moreover, participants' privacy setting decisions in the no cues condition were more open than in the strict condition but less open than in the open cues condition (see Figure 3).

H2 predicted that participants would select more open privacy settings when eye primes were present than when they were not present in the strict cues condition. In contrast to H2, eye primes failed to affect privacy setting behavior in the strict cues condition [$F(1,28) = 1.61$, $p = 0.22$]. However, the means went in the expected direction whereby participants selected more open settings when eye primes were present than when they were absent in the strict cues condition (see Figure 3).

Effects of Privacy Settings on Disclosure Behavior

Participants' disclosure behavior was analyzed by merging the data from Studies 2 and 3 together, and then entering the merged data into a linear mixed model in SPSS v19 where disclosure behavior (frequency or accuracy) was entered as the dependent variable, and order of behaviors (selecting privacy settings first versus filling out a profile first) was entered as the independent variable.

H3 predicted that participants would disclose more inappropriate information if they select privacy settings before filling out a profile in this context. Consistent with H3, participants disclosed more inappropriate information when they selected privacy setting before filling out a profile, $F(1,226) = 7.01$, $p < 0.01$. Participants also disclosed more somewhat appropriate information when they selected privacy settings before filling out a profile $F(1,226) = 8.82$, $p < 0.01$. However, participants' appropriate disclosures were not affected by the placement of the privacy setting page relative to the profile page [$F(1,226) = 1.54$, $p = 0.22$] (see Table 6).

RQ1 asked if disclosure accuracy would be affected by asking participants to select privacy settings before filling out a profile. Disclosure accuracy was unaffected by the placement of the privacy settings page for inappropriate [$F(1,226) = 0.12$, $p = 0.73$], somewhat appropriate

[$F(1,217) = 0.33$, $p = 0.57$], and appropriate [$F(1,219) = 1.61$, $p = 0.21$] information, suggesting that participants did not increase their accuracy as a result of having additional control.

Individual Difference Variables

The following set of analyses focus on how the individual difference variables affect participants' privacy setting decisions.

H4 predicted that high self-monitors are more likely to select privacy settings that follow contextual cues than low self-monitors. A mixed model with privacy settings as the dependent variable, and contextual cues and the self-monitoring factors as independent variables, revealed that, in contrast to H4, neither of the self-monitoring factors influenced participants' privacy setting decisions in the strict, open, or no cues conditions.

H5 predicted that participants with higher levels of digital privacy literacy are less likely to select open privacy settings. A mixed model with privacy settings as the dependent variable, and contextual cues and the digital privacy literacy factors as independent variables, revealed that, in contrast to H5, neither of the technical familiarity, surveillance practices, and policy understanding influenced participants' privacy setting decisions.

Eyes Mechanism

The following set of analyses focus on whether the eye primes had direct or indirect effects.

RQ2 asked if eye primes affect participants' ability to recall details about the SNS and/or recall the indicated norms contained in the contextual cues. The eye primes did not affect participants' ability to answer the detail questions correctly (See Table 7). The eye primes also did not affect participants' ability to answer the norm questions correctly (See Table 7).

Discussion

The primary goal of Study 3 was to examine how contextual cues and eye primes affect privacy setting behavior, while a secondary goal was to examine whether placing the privacy settings page before the profile page affects disclosure behavior. The contextual cues indicating how others had selected their privacy settings affected participants' privacy setting behavior as expected. When the cues indicated a strict privacy setting norm, participants selected stricter settings relative to when the cues indicated an open privacy setting norm. It was expected that eye primes would affect how strict participants would set their privacy settings given that the cues were counter-intuitive to the entrenched (open privacy setting) norm. Although the means were in the expected direction, eye primes did not affect participants' privacy setting decisions in the strict condition. Finally, participants disclosed more information when the privacy settings page came before the profile page, suggesting that placing the privacy setting before the profile page can affect disclosure behavior in SNS contexts. These findings have important implications for Nissenbaum's (2010) framework of contextual integrity and our understanding of the relationship between privacy setting and disclosure behavior.

Implications for the Framework of Contextual Integrity

Nissenbaum's (2010) framework of contextual integrity posits that informational norms, which are determined by contextual cues, prescribe what kinds of information are appropriate to share in a given context. Transmission principles, one of the key contextual cues, place constraints on the distribution and/or dissemination of information from party to party within a context, prescribing when the transfer or sharing of information is appropriate. Privacy settings are designed to be the technical embodiment of transmission principles on SNSs, regulating who can access and share a user's disclosures on and off these sites. Although Nissenbaum (2010) originally conceptualized her framework around disclosure behavior, this study found that

contextual cues can affect privacy setting decisions, which means these kinds of cues can be used to help SNS users abide by informational norms in a SNS contexts.

Ensuring Transmission Principles. Past studies have found that users typically select open privacy settings when they begin using a SNS partially because they perceive other users are also selecting open privacy settings (Lampe et al., 2007). Given that users disclosed according to entrenched disclosure norms in Study 2, we expected participants to select open settings in accordance with entrenched privacy setting norms in Study 3. However, users tended to select stricter privacy settings that would only allow other Cornell students to access their disclosures in this context. This is puzzling considering that newcomers should prefer open settings that help them connect with other users, as well as help them build their network, in SNS contexts. Instead, these findings echo more recent studies that have found users typically select stricter privacy settings so that they can control who can access their disclosures on a SNS (Madden, 2012; Madden et al., 2013; Stutzman, Capra, & Thompson, 2011; Tufekci, 2012; Young & Quan-Haase, 2013). This suggests that participants in Study 3 selected privacy settings that would give them more control over who could access their disclosures, rather than select privacy settings that could help them be found, in this context.

Perhaps participants selected stricter privacy settings so that they could ensure their future disclosure behavior would uphold relevant transmission principles in this context. For example, transmission principles proscribe students from disclosing information with sensitive attributes (i.e., information that could get them in trouble with their T.A.) because the T.A. cannot be trusted to withhold a student's sensitive disclosure from their professor. Let's imagine that a student who joins Cornell Campus Connect selects stricter settings so that he can control who can access his disclosures on the site. This gives him the perception that he can disclose

sensitive information freely on the site without worrying his T.A. will share his disclosures with his professor because the stricter ("Cornell Students Only") setting implies that only his friends and fellow classmates will search for his profile and/or access his disclosures on the site. In other words, selecting stricter setting enhances the perception that relevant transmission principles will be upheld if/when a user desires to disclose sensitive information on a SNS. This also suggests that participants may have anticipated they would want to disclose sensitive information on the site in the future, and wanted to be able to control who could access their disclosures in this context. However, before delving into how privacy settings influenced participants' disclosure behavior, we need to examine how contextual cues influenced participants' privacy setting decisions.

Cues We Can Use. Given that SNSs do not typically provide any information on other users' privacy setting behavior, but users still attempt to determine privacy setting norms via their friends (Lewis et al., 2008; Utz & Kramer, 2009), Study 3 examined if cues indicating privacy setting norms would affect privacy setting behavior in a SNS context. The "strict cues" contained histograms indicating most users had selected strict privacy settings, and the "open cues" contained histograms indicating most users had selected more open privacy settings. In other words, the strict and open cues provided normative information by indicating how strict or open other users had set their settings in this context. Participants selected stricter settings when there were strict rather than open cues on the privacy settings page, suggesting that participants interpreted the strict cue as a behavioral prescription that they *should* select stricter privacy settings in this context. In light of these findings, the framework of contextual integrity may need to be broadened to include privacy setting decisions.

Privacy settings are a technical embodiment of transmission principles; they place constraints on who can access and share users' disclosures on SNSs. However, transmission principles do not exist in a vacuum; they are affected by other contextual cues that indicate if one can disclose a piece of information without worrying it will be shared with unauthorized third parties. Referring to the example above, the student knows he cannot trust the T.A. not to share his sensitive disclosure because the T.A.'s role as an authority figure implies he must share disconcerting information about his students with the professor. On SNSs, users select strict privacy settings to ensure specific others (e.g., T.A.s, professors, parents, etc.) will not be able to see and share their disclosures with others on and off the site. This suggests that privacy setting decisions are susceptible to other key cues that indicate how strict a user should select their privacy settings. As a result, Nissenbaum should include privacy setting decisions into her framework given that, similar to disclosure behavior; privacy settings can affect users' ability to uphold informational norms on SNSs as well as other online contexts.

Eye Primes & Privacy Setting Norms

Study 3 attempted to uncover if eye primes increase behaviors that are consistent with entrenched norms when contextual cues prescribe counter-intuitive behaviors. For example, eye primes increased how much information participants disclosed in this context when contextual cues indicated a norm that most users do not disclose frequently in Study 2, suggesting that eye primes are especially effective in the presence of other cues that run counter-intuitive to the norms that are entrenched in a given context. Given that previous studies have found users tend to select open privacy settings when they initially join a SNS, we expected that eye primes would increase the strictness of participants' privacy setting selections when contextual cues indicated a strict privacy setting norm. However, eye primes did not significantly affect participants' privacy

setting decisions when strict cues were also present on the privacy settings page, although the means were in the expected direction (see Figure 3). This raises the question, why did eye primes fail to affect privacy setting decisions in Study 3?

Perhaps, despite all the studies that have found users select open privacy settings when they initially join a SNS (Ellison et al., 2007; Lampe et al., 2006; 2007), selecting open privacy settings is not an entrenched norm in SNSs. Participants may have selected open settings when these sites first started to gain popularity because they were unfamiliar with the context collapse and default settings that risked their privacy on these sites (Marwick, 2011). Moreover, given that users' select stricter privacy settings as they become more familiar with these sites (Stutzman et al., 2013) suggests that users do not select privacy settings according to norms, but rather select privacy settings according to their experience with the site. This is likely because privacy setting norms are more difficult to decipher (Lewis et al., 2008; Utz & Kramer, 2009) than disclosure norms (McLaughlin & Vitak, 2012) on SNSs. If this is the case, then the eye primes could not affect privacy setting decisions because there are no entrenched privacy setting norms to date.

The Privacy Paradox Replicated

Study 3 also explored if, consistent with the privacy paradox, participants would disclose inappropriate (i.e., information that has been evaluated as too sensitive for this context) information more often after selecting privacy settings in this context. The privacy paradox posits that users who feel they have more control over who can access their information proceed to disclose more sensitive information in an online context (Barnes, 2006; Brandimarte et al., 2013). Study 3 required participants to select privacy settings before filling out a profile, giving them an enhanced sense of control over their information prior to disclosing information on their

profile. We found that participants disclosed information that was perceived as inappropriate and somewhat appropriate for this context more often if they selected privacy settings before filling out a profile, suggesting that the enhanced control they felt over who could access their information led them to feel more comfortable disclosing sensitive information in this context. This seems intuitive because selecting strict privacy settings enhances the perception that a user is placing appropriate constraints on who can access their disclosures on a SNS, lulling users into believing they can disclose sensitive information on the site without worrying if it will be seen by unauthorized (i.e., inappropriate) third parties. However, strict privacy settings do not keep SNS owners from releasing a user's information to advertisers, nor do they keep a user's friends from sharing their information with unauthorized third parties (Brandimarte et al., 2013). Therein lies the paradox: the enhanced feeling of control, triggered by strict privacy settings, increases how much users' disclose sensitive information on SNSs, when in actuality their strict settings do not bar unauthorized others from seeing and potentially sharing what they disclose on these sites. This study found that something as simple as placing the privacy settings before the profile page enhances the perception of control thereby influencing users to disclose sensitive information in this context, increasing the likelihood it will be perceived as inappropriate by other users of the site. This suggests that SNSs are designed almost with the intention of getting users to violate informational norms (e.g., don't disclose sensitive information to a stranger) they would otherwise follow in other contexts.

Individual Differences & Eyes Mechanism.

Similar to Study 2, the individual difference factors and eye prime mechanism measures did not explain any of the privacy setting decisions or disclosure behavior effects in Study 3. As a result, exploring why the individual difference factors failed in both studies will be reserved for

the general discussion. In addition, the lack of eye prime effects in Study 3 leave it unclear as to whether eye primes have direct or indirect effects. However, the findings from Study 2 potentially suggest eye primes may have directly affected participants' disclosure behavior. This will be discussed in greater detail below.

General Discussion

The overall goal of this dissertation was to examine how users can be made aware of and influenced to follow informational norms on SNSs. Study 1 found that university students perceived information with sensitive attributes (e.g., social security number) as less appropriate to disclose on a university-affiliated SNS than information with less sensitive attributes (e.g., academic major). Study 2 explored how contextual cues indicating disclosure norms and eye primes influence users' disclosure behavior on a SNS and found that when contextual cues indicated a low disclosure norm, participants disclosed less information than when cues indicated a high disclosure norm. The eye primes influenced how often and how accurately participants disclosed in this context than when eye primes were not present in the low disclosure condition specifically, suggesting that the eye primes were increasing disclosure behaviors that are entrenched as normative in SNS contexts.

Study 3 explored how contextual cues and eye primes influence users' privacy setting decisions and subsequent disclosure behavior and found that when contextual cues indicated a strict privacy setting norm, participants selected stricter settings than when contextual cues indicated an open privacy setting norm. The eye primes did not affect participants' privacy setting decisions. Placing the privacy setting page before the profile page led participants to disclose information perceived as inappropriate and somewhat appropriate for this context more

frequently in Study 3 than when the profile page came before the privacy settings page in Study 2.

Finally, Studies 2 and 3 found no individual difference effects, nor did the eyes mechanism measures demonstrate whether the eye primes were directly or indirectly affecting participants' disclosure behavior and/or privacy setting decisions.

Theoretical Contributions

Nissenbaum's Framework of Contextual Integrity. These results have several important implications for Nissenbaum's (2010) framework of contextual integrity. First, while many scholars have used Nissenbaum's (2010) framework as a lens to help them understand user disclosure behavior in online contexts (Debatin, 2011; Cohen, 2013; Heeney, 2012), this is one of the first empirical tests of her framework in a SNS context. This empirical test produced behavioral data consistent with Nissenbaum's (2010) framework, with the results from Studies 2 and 3 indicating the Contextual Integrity framework can be used to predict and explain users' disclosure behaviors and privacy setting decisions in SNS contexts. Lastly, the finding that eye primes increased disclosure frequency and accuracy suggests that nonconscious cues can influence whether or not people abide by informational norms they typically follow in similar contexts. The second and third implications will be discussed in greater detail below.

There were some asymmetries in the data that were not anticipated by the Contextual Integrity framework. For example, the low disclosure norm cue decreased disclosure frequency, but the high disclosure norm did not did not increase disclosure frequency (see Figure 1). Similarly, the strict privacy setting cue seemed to be more effective at getting participants to select stricter settings than the open privacy cue's ability to affect how open participants set their privacy settings (see Figure 3). Taken together these data suggest that SNS users are influenced

more by cues that encourage privacy-oriented behaviors rather than cues that encourage risky information sharing behaviors.

Why is it the case that, overall, our participants were more likely to follow contextual cues that prescribe privacy oriented behaviors? Past research has found that users are concerned about their privacy on SNSs, yet still engage in behaviors that put their privacy at risk (Stutzman et al., 2013). Perhaps this disconnect is a result of users' uncertainty as to how much they should disclose, or how strict they should set their privacy settings, in order to ensure their privacy on these sites. The results of Studies 2 and 3 suggest that giving users contextual cues that show them how other users' protect their privacy can help them follow suit on SNSs. After all, Nissenbaum (2010) contends that explicating informational norms should help users make smarter (i.e., more appropriate) information sharing decisions in online contexts. The overall results of these studies supports her contention, suggesting that adding these kinds of cues to SNSs may help users abide by a site's informational norms, and in turn ensure their privacy, on these sites.

The effects of eye primes on disclosure behavior suggest that the Contextual Integrity framework may need to incorporate how nonconscious cues affect adherence to informational norms in various contexts. Nissenbaum's (2010) framework currently highlights how contextual cues (e.g., aspects of interaction partners, features of the physical context, etc.) determine relevant informational norms, which subsequently influence disclosure behavior in a given context. However, the cues she describes tend to be rather apparent or salient, implying that these cues need to be consciously perceived before a discloser can follow relevant informational norms. In contrast, the eye primes, which increased how often and accurately participants disclosed information in this context, were never mentioned were never mentioned by

participants in the follow-up survey. These results suggest that nonconscious cues (e.g., psychological primes) can affect people's willingness to abide by relevant informational norms in a given context

Contextual Integrity versus CPM. Results from Study 2 suggest that Nissenbaum's framework is slightly better equipped than Petronio's CPM (2002) at uncovering how users make initial disclosure decisions on SNSs (e.g., profile creation). Recall that Petronio (2002) posits that privacy rules can sometimes be routinized and habitually followed in a given context. The finding that participants disclosed frequently and accurately in this context is consistent with Petronio's (2002) routinization contention; participants seemed to apply general informational norms or privacy rules that influence disclosure frequency and accuracy on other SNSs to this context. However, the contextual cue findings are more consistent with Nissenbaum's (2010) framework. The contextual cues indicated norms or rules that were contrary to how users routinely disclose information in SNS contexts. The finding that these cues disrupted routine disclosure patterns underscores how powerful contextual cues can affect users' disclosure behavior in SNS contexts. This should not suggest that Petronio's (2002) CPM cannot explain other ways users manage their privacy on SNSs, such as how users determine when a private disclosure is perceived as inappropriate in SNS contexts.

Although Nissenbaum's (2010) framework helps us predict when users might disclose versus withhold sensitive information, Petronio's (2002) CPM may be better at predicting when sensitive information is perceived as inappropriate after it is disclosed or shared in a given context. According to Petronio (2002) boundary turbulence occurs when sensitive information is shared with unauthorized third parties. The findings from Study 1 suggest that sensitive information has the potential to be perceived as inappropriate in public SNS contexts. This is an

important distinction, sensitive information is not perceived as inappropriate until unauthorized third parties become privy to that sensitive information. This is likely why participants did not disclose sensitive information frequently or accurately in Studies 2 and 3; they wanted to avoid the possibility that an unauthorized third party would see their sensitive disclosure(s). By withholding sensitive information, they attempted to ensure that their disclosures would be perceived as appropriate, thereby avoiding the occurrence of boundary turbulence. However, sometimes participants did disclose sensitive information in this context (Study 3), putting themselves at greater risk for encountering boundary turbulence (i.e., that unauthorized third parties would see their private information), suggesting that Petronio's (2002) CPM may help predict when and how disclosure behavior results in informational norm violation, or privacy boundary turbulence, in SNS contexts.

Context Collapse. While the results of Studies 2 and 3 are consistent with Nissenbaum's (2010) general contention that people use contextual cues to determine what is appropriate to disclose in a context, these results also suggest some important limitations of the framework when applied to SNS contexts. Nissenbaum (2011) contends that the framework helps users "locate contexts, explicate entrenched informational norms, identify disruptive flows, and evaluate these flows against norms" that help determine if an informational norm is upheld or violated in an online context (p. 38). Offline informational norms are relatively easy to follow given that people can typically identify contextual cues that indicate the entrenched informational norms. For example, in a university building hallway, it is easy for a student to detect if their professor is nearby, which will then indicate if disclosing about their Caribbean cruise is or is not appropriate. However, on SNSs it is not as easy to detect who else can see a user's disclosures given that SNSs typically *collapse* into a single heterogeneous context

(Marwick & boyd, 2011). For example, the Facebook Newsfeed tends to display posts from users one frequently interacts with on the site, heightening the perception that only those who pop up in their Newsfeed will likely see their Facebook posts (Debatin, Lovejoy, Horn, & Hughes, 2009). This aspect of Facebook's design leads users to forget how multiple contexts (e.g., a user's friends, family, classmates, and professors), not just the ones who pop up in their Newsfeed, can see and access their posts on the site. As a result, it can be difficult for users to locate which contexts are relevant, and determine which informational norms they need to abide by when disclosing on SNSs.

Context collapse can lead users to violate their own and others' privacy unwittingly, suggesting that they are unable to detect or determine the contextual cues that indicate appropriate disclosure behavior in SNS contexts (Hull et al., 2011; Litt et al., 2014; Marwick, 2012). For example, Wang and colleagues (2011) found that one of the main reasons users regret disclosing sensitive information on Facebook was because they forgot their public disclosures could be seen and shared by unintended third parties, suggesting that users have difficulty applying informational norms to SNSs because the necessary contextual cues are obscured. Providing users with simple cues that indicate a site's informational norms may help users ensure their disclosures are appropriate for a SNS context, consistent with the results from Study 2 where participants disclosed less information when contextual cues indicated that they should not disclose a lot of information on their profiles. In summary, Nissenbaum's (2010; 2011) framework of contextual integrity has difficulty accounting for context collapse, and that contextual cues such as the ones used in Studies 2 and 3 may be able to help users abide by relevant informational norms in a SNS context.

Privacy (Paradox) by Design. According to the privacy paradox (Barnes 2006; Brandimarte et al., 2013), the more control users feel they have over their information, the more likely they are to disclose sensitive information in an online context, even though having more perceived control does not necessarily mean a user's information is adequately protected (Brandimarte et al., 2013). For example, recent research has found that users who select stricter settings tend to disclose more sensitive information on SNSs (Stutzman et al., 2013), suggesting that users who select stricter privacy settings feel they have more control over who can see what they disclose on the site. Moreover, users who exert this control by selecting stricter settings by limiting likely perceive that it is appropriate to disclose sensitive information on SNSs because they have limited access to those they trust with their sensitive information. Study 3 found that asking users to select privacy settings before filling out a profile prompted users to disclose sensitive information, suggesting that giving users the ability to exert control over their information prior to filling out a profile may lead them to perceive whatever they disclose on their profile will be effectively protected by their privacy settings. However, neither the granularity of a site's privacy settings, nor the placement of the privacy settings page, keep a user's contacts and/or keep the site's owners from sharing their information with third parties. This suggests that users overestimate how effective privacy settings are at helping them uphold relevant transmission principles in SNS contexts, and increases the risk that their sensitive disclosures will be perceived as inappropriate by unauthorized third parties.

Transmission principles indicate when it is appropriate for a person to share a piece of information with another person or group of people in a given context (Nissenbaum, 2010). Privacy settings are meant to place constraints on who can access and share a user's disclosures on a SNS. However, SNS privacy settings may not effectively constrain unauthorized third

parties from accessing and sharing user information on and off these sites. For example, users who select "Friends Only" setting for their "Who can see my profile?" privacy setting likely assume that only those in their network can access their profile on Facebook. However, while Facebook's privacy settings place constraints on which users can access a user's profile, they do not constrain Facebook from sharing users' profile disclosures with unauthorized third parties (e.g., advertisers). If users were aware of Facebook's sharing practices, they might refrain from disclosing sensitive information such as their hometown and phone number on their profile because they are not sure whether third-parties will take advantage of their information (Stutzman et al., 2013). Moreover, SNS privacy policies tend to be exceedingly long as well as incomprehensible (Fuchs, 2012; Grimmelmann, 2008), making it difficult for users to determine if their privacy settings are placing the appropriate constraints on who can access and share their information on SNSs. Given that SNSs such as Facebook have granular privacy settings and complicated privacy policies, it is possible that these sites are designed to lead users into thinking their privacy settings are placing appropriate constraints on who can access and share their information (Zimmer, 2008).

SNSs such as Facebook claim that their primary motivation "is to give people the power to share and make the world more open and connected" (Facebook, 2014). However, given that they also sell user data to third-parties (e.g., advertisers), they also have strong economic motivations as well (Fuchs, 2012; Stutzman et al., 2013; van Dijck, 2013). For example, Facebook's design gives users ample opportunities to disclose information on their profiles, via public and private messages, as well as liking and commenting on other users' posts. Although Facebook's privacy settings can constrain users' ability to see and share each other's disclosures, they do not constrain Facebook's ability to share their data with third parties (Fuchs, 2012).

When users accept Facebook's Terms of Service, they "agree to the use of their self-descriptions, uploaded data, and transaction data to be sold to advertising clients" (Fuchs, 2012, p.11). In other words, Facebook reserves the "right" to sell users' profile disclosures, status updates, photos, likes, comments, etc. to advertisers (van Dijck, 2013). The more users' disclose, the more data Facebook can sell to advertisers, suggesting that Facebook as well as other SNSs are economically motivated to get users to share as much information as possible. As a result, SNSs design their communication features and privacy settings to get users to disclose as much as possible on their sites. Given their economic interests, SNSs are unlikely to add contextual cues (similar to those used in Studies 2 and 3) that inform users about their sites' informational norms because doing so might diminish their bottom line.

Eye Primes and Behavioral Representations. Although the eye primes did not affect participants' ability to answer questions about the site in the post-study survey, their effects on disclosure frequency and accuracy suggest they may have directly affected their disclosure behavior. According to Ferguson and Bargh (2004), "behavioral representations can be automatically activated in memory during perception, and, once activated, can guide actual behavior" (p. 34). Given that eye primes heighten the perception that "one's actions are being observed" (Haley & Fessler, 2005, p. 249), eye primes may activate behavioral representations that adhere to the norms entrenched in a context in order to garner the liking and approval of an "observer". In other words, they should make behaviors that are geared towards obtaining others' liking and approval more accessible, suggesting that eye primes should increase disclosure frequency and accuracy in a SNS context because these disclosure behaviors are not only expected but also associated with obtaining other users' liking and approval on a SNS (Lampe et al., 2006).

This mechanism can also explain why the eye primes increased how often and how accurately participants' disclosed information in this context relative to when there was a control image in the low cues condition specifically. The low contextual cue indicated a low disclosure norm to the user, suggesting that the user should not disclose much information in this context. When there were no eye primes present, participants followed the norm indicated by the low contextual cue and disclosed less information. However, when eye primes were present in the low cue condition, participants disclosed more often and more accurately, possibly because the eye primes activated disclosure behavior representations associated with obtaining other users' approval and liking, making disclosure frequency and accuracy more accessible and available in this context. Moreover, the eye primes did not increase disclosure frequency and accuracy when there were no contextual cues because participants were already following the entrenched norm. Disclosing frequently and accurately is expected on SNSs generally, implying these disclosure behaviors were already accessible in participants' minds when they began filling out their profile. This would also explain why eye primes increased how often patrons picked up their litter in a cafeteria context (Ernest-Jones et al., 2011). Picking up litter is not only expected in a cafeteria context, doing otherwise risks' appearing lazy and dirty in front of other patrons. If eye primes activate behavioral representations associated with obtaining an observers' liking and approval, patrons may have picked up litter more often when eye primes were present than absent because the primes activated behavioral representations associated with obtaining other (observing) patrons' approval in a cafeteria context. The results of these studies suggest that eye primes activate behavioral representation associated with entrenched norms, making these behaviors more accessible and thus easier to perform in a given context.

Future Research

Individual Differences and Privacy Behaviors. Individual difference factors did not explain users' disclosure behavior or privacy setting decisions in either Study 2 or 3. Why did these factors fail to influence any of the privacy behaviors? Consider first self-monitoring. Other recent work suggests that high self-monitors do not always follow salient norms. In his study of South Korean drinking behaviors, Jang (2012) found that, although high self-monitors perceived a salient norm that prescribed frequent alcohol consumption, they did not drink according to the norm. Moreover, Jang (2012) suspected this effect was due to high self-monitors being more concerned with their friends' drinking behaviors rather than salient, and somewhat ambiguous, drinking norms. This suggests that high self-monitors may be more inclined to follow norms that their friends endorse rather than norms that are entrenched in a context generally. Future research should explore if self-monitors would be more likely to follow norms their friends endorse to see if individual levels of self-monitoring can affect the ways users share information on these sites.

Although digital privacy literacy did not explain users disclosure behavior or privacy setting decisions, they may still be able to explain users privacy-oriented behaviors on SNSs. One of the possible reasons why digital privacy literacy did not affect users disclosure behavior and/or privacy setting decisions may be because of this context's apparent affiliation with an institution participants could trust: Cornell University. In a study examining what influences users to disclose information on commercial websites, Metzger (2004) found that regard for the company and trust in the website were both positive predictors of disclosing identifying information on her study's site. Moreover, the site used in her study was practically identical to an actual commercial website (only the name was changed). This suggests that users may be more willing to disclose information on a website if the site looks official and/or familiar. The context used in Studies 2 and 3 was made to appear as though it was officially associated and

overseen by researchers at Cornell University (see Appendices A-C). This context contained the official Cornell logo, Cornell colors (red and white), pictures and images of Cornell campuses and buildings, etc. As a result, participants may have assumed that whatever they disclosed in this context would be safe given its affiliation with their university.

If this were the case, then a participant's level of digital privacy literacy may have been irrelevant because of the study's affiliation with the participant's university. Perhaps if this context was broader in terms of user base and purpose, participants high in this trait may have been more reluctant to disclose their information, or more inclined to select stricter settings, because they would be unsure if they could trust the owners of the site not use or share their data in inappropriate ways. Future research should explore how digital privacy literacy affects disclosure behavior and privacy setting decisions in more diverse and/or large SNSs to see how this individual difference affects information sharing behavior on these sites.

Goals and Self-Disclosure. People follow informational norms for a reason. That is, people follow norms so they can ensure what they disclose is appropriate for the context, maintain a pleasant social atmosphere, and hopefully obtain the liking and approval of others in a given context. This implies that adhering to informational norms is inherently goal driven. Moreover, similar to informational norms, the activation and pursuit of social goals can be affected by features of, or apparent cues in, a given context. For example, those who sought a social validation goal via Facebook tended to disclose less sensitive information via public messages (Bazarova & Choi, 2014). This may in part be because Facebook users know that a public message can be seen by more people thus increasing the likelihood of obtaining social validation. However, Facebook users also know that it is inappropriate to disclose sensitive information publicly on the site (Bazarova, 2012). These findings suggest that Facebook users

may adjust their disclosure behavior to fit the informational norms in a context so that they can maximize their ability to obtain a social validation goal.

The contextual cues that contained normative information in this study may have affected how participants pursued social goals via their profile disclosures. SNSs users typically disclose often and accurately on their profiles because these disclosure behaviors are entrenched as normative on these sites. If they disclose according to the norms, they are more likely to obtain social validation as well as other goals they associate with SNSs (getting found by relevant others on the site, building their network, etc.). However, when contextual cues indicated a low disclosure norm in this context, participants disclosed less information on their profiles, likely because they thought violating the norm would undermine their social validation goal. This is because violating norms, informational and otherwise; typically result in social sanctions rather than social rewards (Burgoon, Parrott, Le Poire, Kelley, Walther, & Perry, 1989). Future research should explore how adhering to informational norms may partially be driven by social goal pursuit in SNS as well as other contexts.

Limitations

There are several limitations to this study that need to be addressed. First, although the site designed for this study was made to resemble other actual SNSs, participants likely perceived that this site was designed for the purposes of an experiment rather than a SNS they would actually use. While this raises concern that they may have disclosed in ways they perceived would please the researchers, their disclosure behavior mollifies this concern. For example, if participants perceived the researchers wanted them to disclose more information when contextual cues indicated a high disclosure rate of around 70% they would have tried to ensure their disclosure behavior matched the high contextual cue. Instead, participants'

disclosure rates in the high cues condition hovered around 55% in Studies 2 and 3, suggesting they were not trying to disclose according to how much they perceived the researcher wanted them to disclose. This suggests that participants were treating this as a hypothetical SNS rather than an actual SNS.

Another limitation is the sample population. This study's use of an undergraduate population was deliberate given our research goals. For example, depicting the SNS as affiliated with the participants' university helped us predict and examine how users make information appropriateness evaluations (Study 1), which in turn allowed us to explore how contextual cues and eye primes affected their disclosure behaviors (Study 2) and privacy setting decisions (Study 3). However, given that SNSs such as Facebook are incredibly diverse regarding users' age, ethnicity, education as well as income levels (Duggan & Brenner, 2013; Lee, 2012); the generalizability of these studies' findings is limited. Given user diversity is typical on SNSs such as Facebook, it is likely that SNS users have different perceptions of disclosure appropriateness and may be more or less susceptible to contextual cues indicating disclosure norms as well as the normative effects of eye primes. For example, while younger US users may perceive disclosing their relationship status is appropriate for Facebook, older South Korean users may perceive disclosing their relationship status is inappropriate for Facebook given the latter culture's emphasis on privacy and respectfulness (Sung, 2004). Future research should explore how contextual cues and eye primes affect disclosure behavior and privacy settings decisions on larger SNSs to see if the contextual cues and eye prime effects hold for more diverse populations.

Conclusion

Consistent with Nissenbaum's (2010) framework of contextual integrity, contextual cues can affect users' information sharing behavior on SNSs, and influence the likelihood they will engage in privacy-oriented behaviors on these sites. In addition, the eye primes findings suggest that eye primes do not increase normative behaviors generally, but instead increase normative behaviors that may help people obtain others' approval and liking in a given context. Finally, consistent with the privacy paradox (Brandimarte et al., 2013), subtle changes such as placing the privacy settings page before the profile page can enhance users' belief they are placing the appropriate constraints on who can access and share their information, increasing the amount of sensitive information they disclose on SNSs. Overall, these results suggest that people strive to adhere to informational norms on SNSs, and that cues, primes, and the placement of pages, can significantly affect the appropriateness, frequency, and accuracy of their disclosures on these sites.

Appendices

Appendix A: Profile Information Survey

Hello and Thank You for participating in this study! I would like you to imagine that Cornell is building a new Social Networking Site designed to help Cornell students from the Ithaca and NYC campuses connect to each other. I want you to think about what kinds of information you think would be appropriate to include in a profile for a Cornell affiliated Social Networking Site? I'd also like you to think whether a given piece of information is more or less private.

Please review the following kinds of information and rate them according to how 1) how **appropriate** it would be share to that information on a Cornell affiliated SNS profile, 2) how **comfortable** you would be sharing that information on a Cornell affiliated SNS profile, 3) how **private** you perceive that piece of information to be, and 4) how **SENSITIVE** you perceive that piece of information to be. Please rate all 42 pieces of information along these four dimensions.

1 (Very Inappropriate) 2 (Kind of Inappropriate) 3 (Appropriate) 4 (Pretty Appropriate) 5 (Totally Appropriate)

1 (Very Uncomfortable) 2 (Kind of Uncomfortable) 3 (Comfortable) 4 (Pretty Comfortable) 5 (Totally Comfortable)

1 (Extremely Private) 2 (Somewhat Private) 3 (Private) 4 (Not That Private) 5 (Not At All Private)

1 (Extremely SENSITIVE) 2 (Somewhat SENSITIVE) 3 (SENSITIVE) 4 (Not That SENSITIVE) 5 (Not At All SENSITIVE)

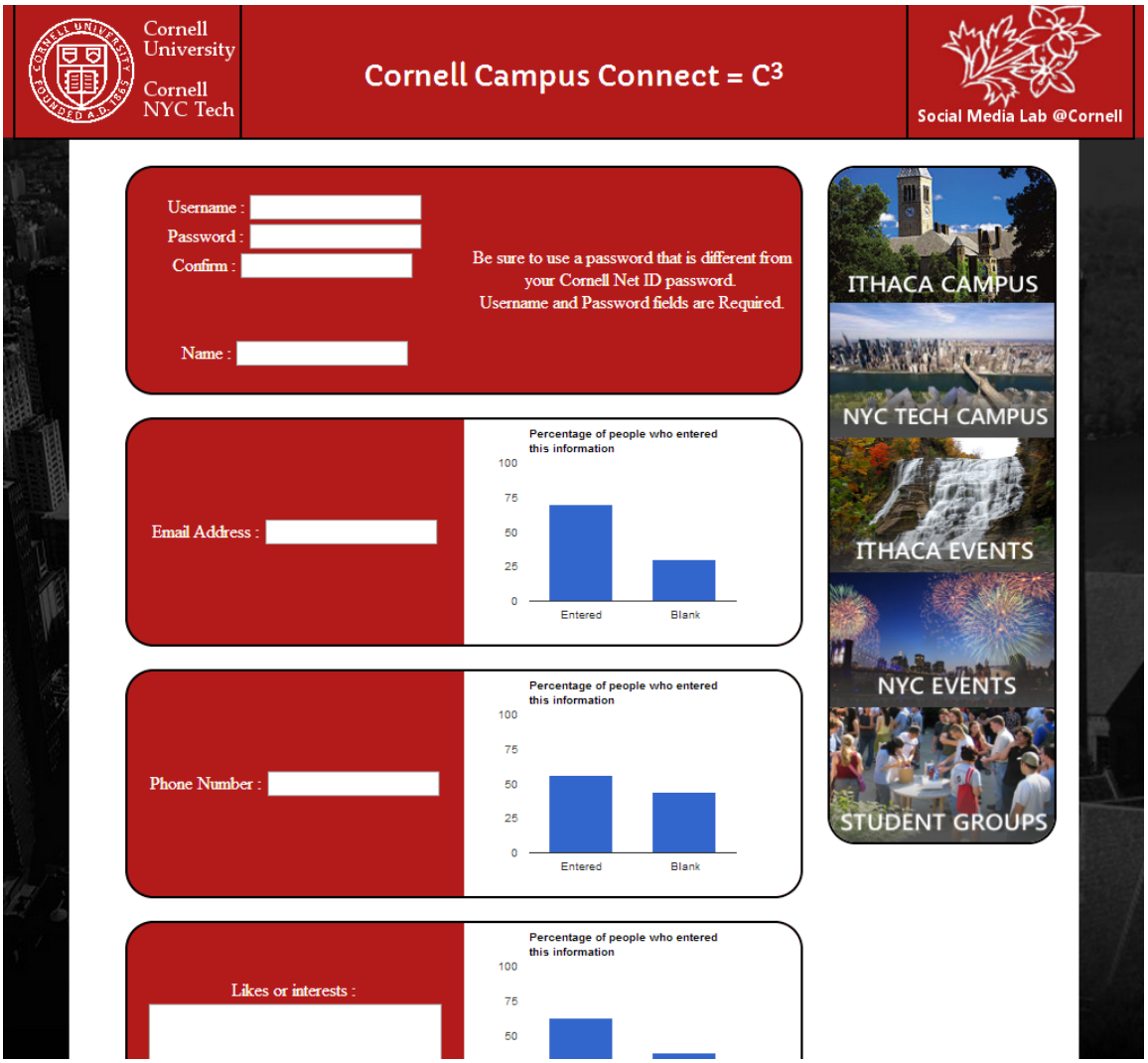
1) Academic Accomplishments
2) Pictures of Friends
3) Athletic Accomplishments
4) Clubs/Organizations That You Belong To
5) College Affiliation
6) Dorm/Off-Campus Housing Area (e.g., Collegetown, Commons, etc.)
7) Educational Networks
8) Fraternity/Sorority
9) Hometown
10) Likes/Interests
11) Email Address
12) Major
13) Extracurricular Activities
14) Permanent Address
15) Cornell Net ID

16) Pictures of Family

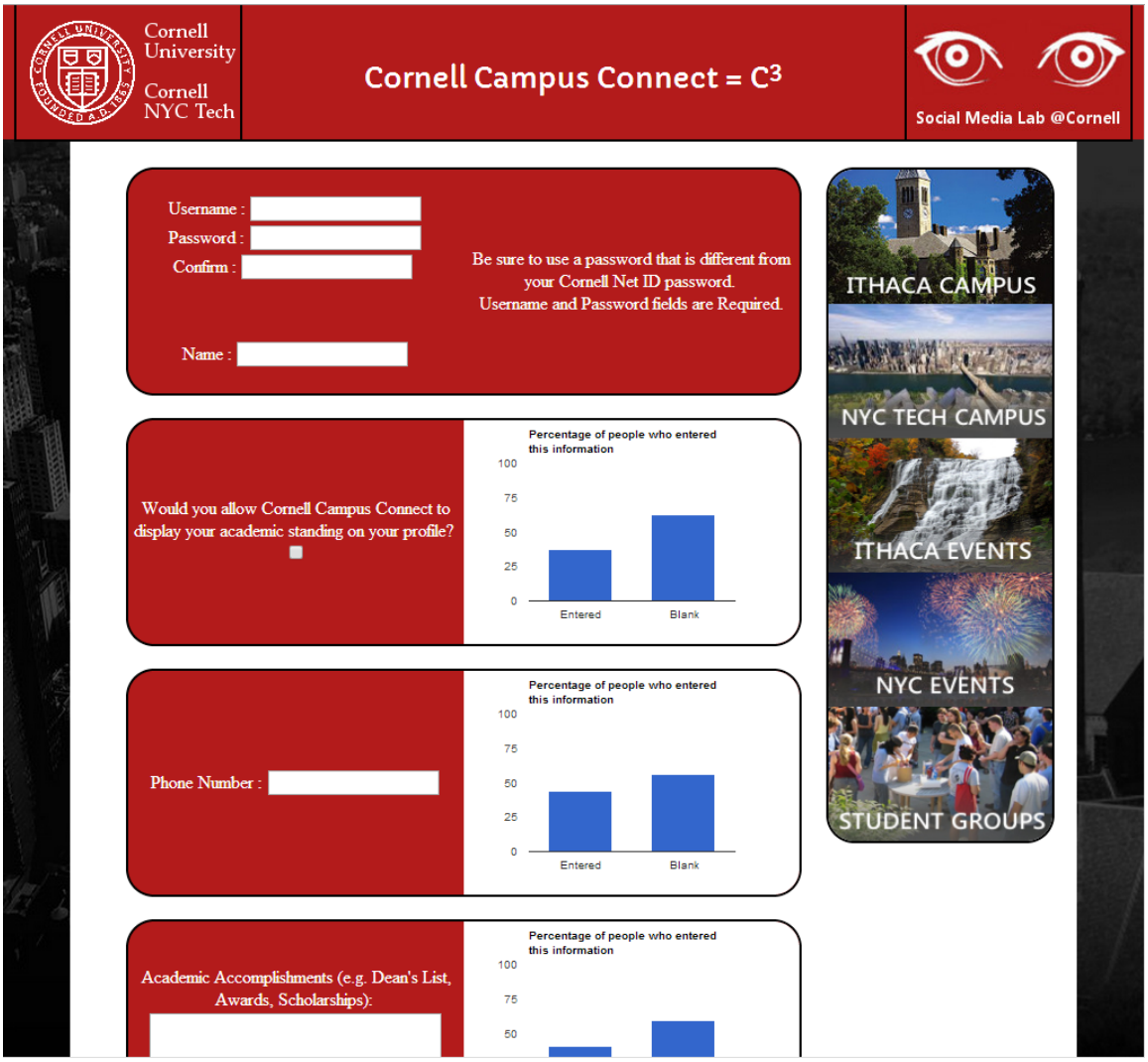
17) Current Address
18) Academic Standing (e.g., Dean's List, Probation, etc.)
19) Graduation Year
20) Social Security Number
21) Your Professor Ratings
22) Pictures of You at Parties, Going Out, etc.
23) Credit Card Information
24) Home Phone Number
25) Secrets
26) Relationship Status
27) Banking Information (e.g., which bank you use)
28) Location Data (e.g., GPS Data)
29) GPA
30) Direct/Private Messages
31) Pictures You're Tagged In
32) Cornell ID #
33) An Emotional Status Update
34) Birthdate
35) Classes Taken
36) Embarrassing Pictures of You and Your Friends
37) Middle Name
38) List of Your Friends
39) Cell Phone Number
40) Medical Information
41) Sexual Orientation
42) Relationship History

Appendix B: Cornell Campus Connect Home Page

Appendix C: Study 2 Contextual Cue Histograms



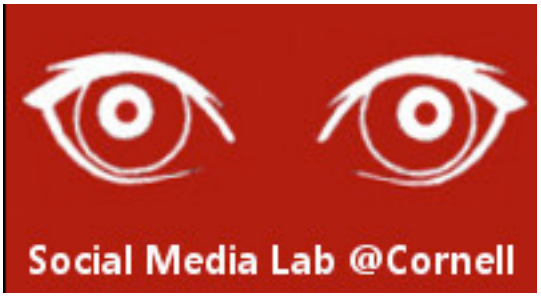
High Cues Condition



Low Cues Condition

No Cues Condition

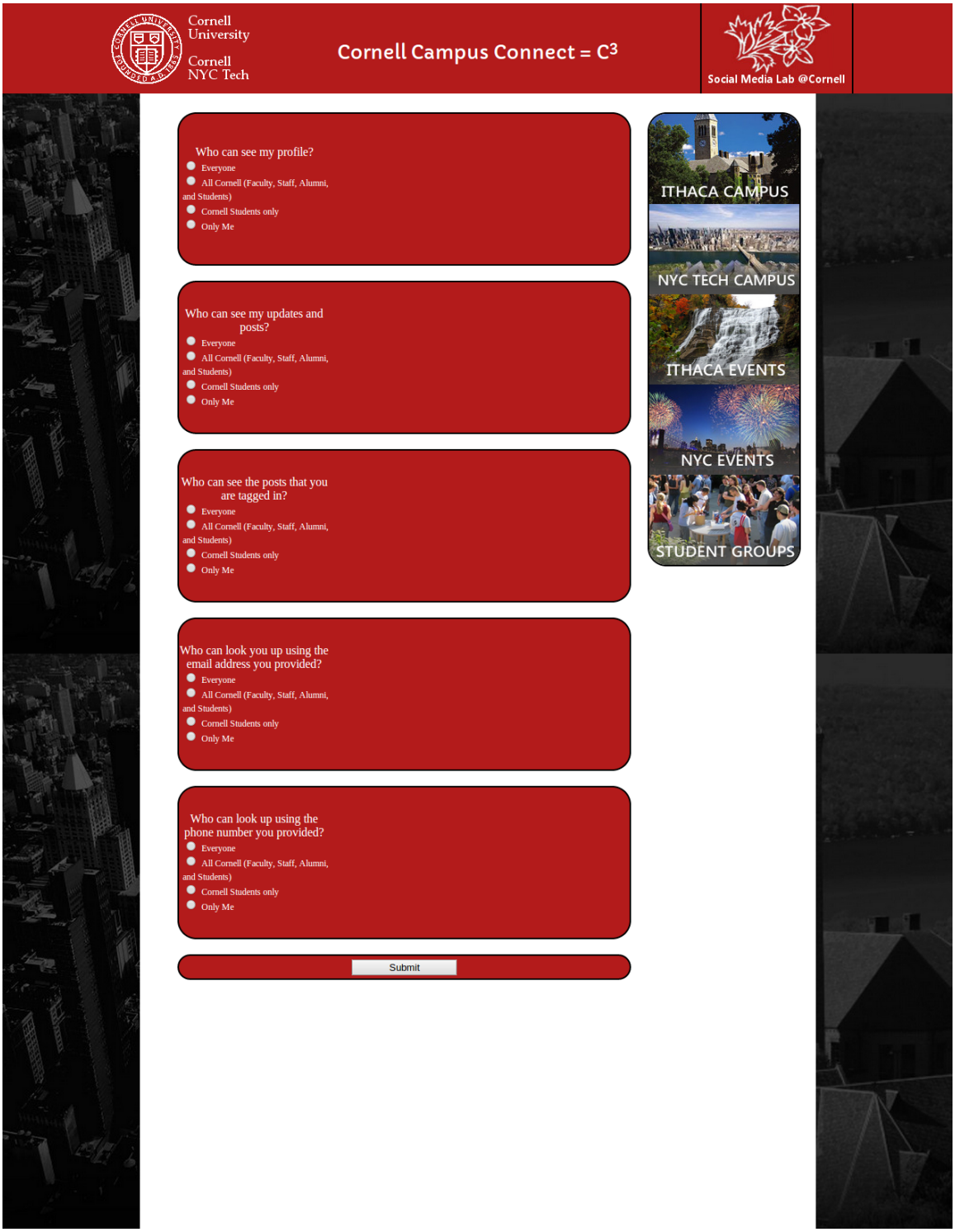
Appendix D: Eye Prime and Control Images



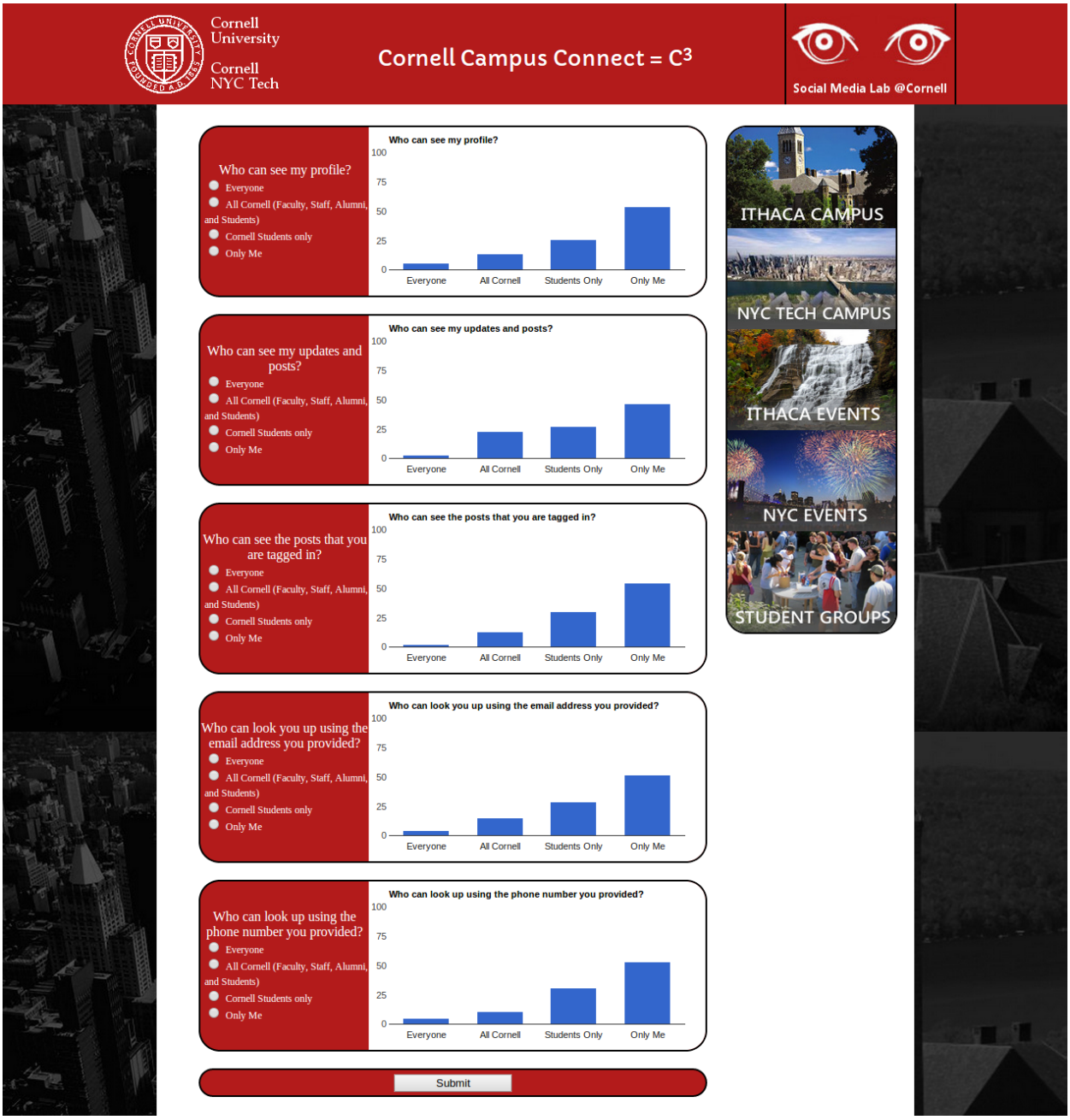
Eye prime

Control image

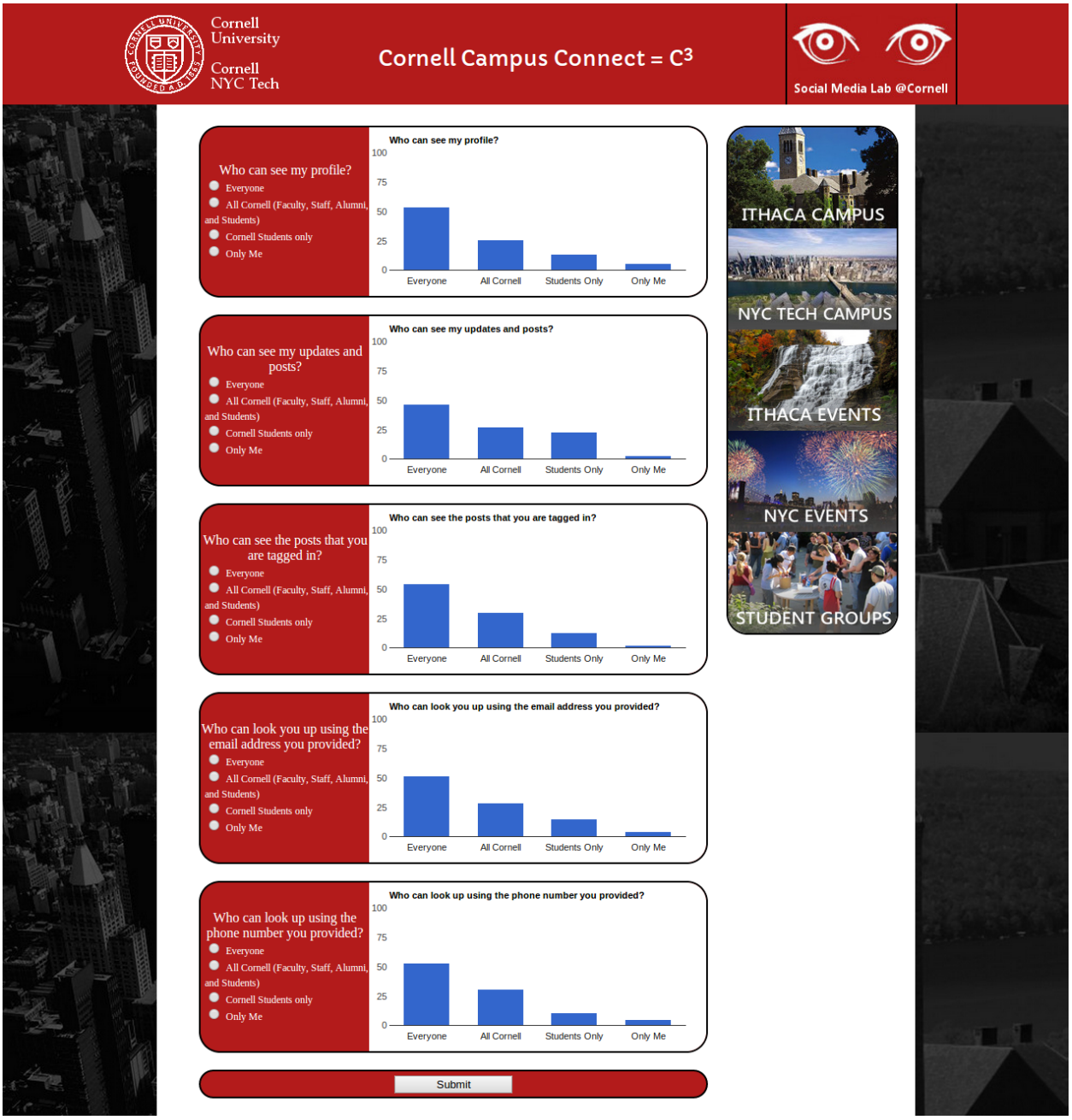
Appendix E: Study 2 Privacy Settings



Appendix F: Study 3 Contextual Cues



Strict Cues Condition



Open Cues Condition

No Cues Condition

Appendix G: Post-Study Survey

Cornell Campus Connect Feedback

Q11) What did you like about Cornell Campus Connect?
Q12) What did you dislike about Cornell Campus Connect?
Q13) What changes should we make to Cornell Campus Connect?

What do you remember about the Cornell Campus Connect pages?

Q1_1) What was the name of the lab that is hosting this network?
a. Social Media Lab
b. Science Methods Lab
c. Social Manifold lab
d. Science and Media Lab

Q1_2) What is the name of the network?
a. Cornell Campus to Campus
b. Cornell City Connection
c. Cornell Campus Connect
d. Cornell College Contacts

Q1_3) What was the color of the site's banner?
a. Green
b. Orange
c. Blue
d. Red

Q1_4) How many users entered their student number into their site profile?
a. All users
b. Most users
c. Few users
d. No users

Q1_5) How many users allowed the site to tag their location to their posts?
a. All users
b. Most users
c. Few users
d. No users

Q1_ 6) How many users entered their address into their site profile?
a. All users
b. Most users
c. Few users
d. No users

Q1_ 7) How many users allow other search engines to link to their profile?
a. All users
b. Most users
c. Few users
d. No users

Q1_8) How many pieces of information we asked about on the profile/login page?
a. 15
b. 5
c. 10
d. 20

Q1_9) How many privacy settings were there?
a. 3
b. 7
c. 15
d. 20

Q1_10. How many users entered their SSN into their profiles?
a. All users
b. Most users
c. Few users
d. No users

Q2: Self-Monitoring Scale

Consider the way you interact with others during face-to-face interactions. Please indicate the extent to which you agree or disagree with the following statements. 1= strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=strongly agree.

Q2_1: I have the ability to control the way I come across to people depending on the impression I wish to give them.
Q2_2: I have found that I can adjust my behavior to meet the requirements of any situation I find myself in.
Q2_3: Once I know what the situation calls for, it's easy for me to regulate my actions accordingly.
Q2_4: If someone is lying to me, I usually know it at once from that person's manner of expression.
Q2_5: I try to pay attention to the reactions of others to my behavior in order to avoid being out of place.
Q2_6: In social situations, I have the ability to alter my behavior if I feel that something else is called for.
Q2_7: I am often able to read peoples' true emotions correctly through their eyes.
Q2_8: In conversations, I am SENSITIVE to even the slightest change in the facial expression of the person I'm conversing with.

Q2_9: My powers of intuition are quite good when it comes to understanding others' emotions and motives.
Q2_10: I can usually tell when others consider a joke to be in bad taste, even though they may laugh convincingly.
Q2_11: When I feel that the image I am portraying isn't working, I can readily change it to something that does.
Q2_12: I have trouble changing my behavior to meet the requirements of the situation I am in.
Q2_13: Even when it might be to my advantage, I have difficulty putting up a good front.

Q3: **Self-Monitoring/Facebook**

Consider the way you interact with others on Facebook. Indicate the extent to which you agree or disagree with the following statements. 1=strongly disagree, 2=disagree, 3=neutral, 4=agree, 5=strongly agree

Q3_1: I have the ability to control the way I come across to people on Facebook depending on the impression I wish to give them.
Q3_2: I have found that I can adjust my behavior to maintain my own and others' impressions on Facebook.
Q3_3: Once I know what the situation calls for, it's easy for me to act accordingly on Facebook.
Q3_4: When I feel that the image I'm portraying on Facebook isn't working, I can readily change it to something that does.
Q3_5: I don't pay attention to my Facebook friends' reactions to my posts and comments on Facebook.
Q3_6: Even when it might be to my advantage, I have difficulty putting up a good front on Facebook.
Q3_7: On Facebook, I have the ability to alter my behavior if I feel that something else is called for.

Q4: Digital Privacy Literacy Scale

Technical Familiarity
Please indicate how familiar you are with the following technologies on a scale from 1 = not at all familiar to 6 = very familiar. (1 = not at all familiar, 2 = slightly familiar, 3= somewhat familiar, 4 = relatively familiar, 5 = pretty familiar, 6 = very familiar)

Q4_1) Generic Internet
Q4_2) HTML
Q4_3_Preference setting
Q4_4) ISP
Q4_5) Cache
Q4_6) BCC (on email)
Q4_7) Privacy risk
Q4_8) Phishing
Q4_9) Privacy protection
Q4_10) p3p

Surveillance Practices
Please indicate if you think the following statements are True or False (True/False)

Q4_11) Companies today have the ability to place an online advertisement that targets you based on information collected on your web-browsing behavior.
Q4_12) A company can tell you that you have opened an email even if you do not respond.
Q4_13) When you go to a web site, it can collect information about you even if you do not register.
Q4_14) Popular search engine sites, such as Google, track the sites you come from and go to.
Q4_15) E-commerce sites, such as Amazon or Netflix, may exchange your personal information with law enforcement and credit bureau.
Q4_16) What a computer user clicks while online surfing can be recorded as a trail.
Q4_17) Most online merchants monitor and record your browsing in their sites.
Q4_18) When a web site has a privacy policy, it means the site will not share your information with other websites or companies.

Policy Understanding
Please indicate if you think the following statements are True or False (True/False)

Q4_19) Government policy restricts how long websites can keep the information they gather about you. *False*
Q4_ 20) It is legal for an online store to charge different people different prices at the same time of day. *True*
Q4_21) A website is legally allowed to share information about you with affiliates without telling you the names of the affiliates. *True*
Q4_22) By law, e-commerce sites, such as Amazon, are required to give you the opportunity to see the information they gather about you. *False*
Q4_23) Privacy laws require website policies to have easy to understand rules and the same format. *False*
Q4_24) U.S. government agencies can collect information about you online without your knowledge and consent. *False*
Q4_25) When I give personal information to an online banking site such as citibank.com, privacy laws say the site has no right to share that information, even with companies it owns. *True*

Q5) Accuracy

Please indicate whether or not the information you entered into your profile is accurate or inaccurate. (Accurate = 1, Inaccurate = 0).

Q5_1) School or College Affiliation
Q5_2) Number of Past Romantic Relationships
Q5_3) Hometown
Q5_4) Cornell Net ID
Q5_5) Academic Major or Field

Q5_6) Email Address
Q5_7) Phone Number
Q5_8) Important Medical Information (e.g., chronic or past conditions, allergies)
Q5_9) Dorm-Off Campus Address
Q5_10) Permanent Address
Q5_11) Would you allow Cornell Campus Connect to display your academic accomplishments on your profile?
Q5_12) Cornell ID Number (7-digit number found on your University ID card)
Q5_13) Club/Student Organization
Q5_14) Relationship Status
Q5_15) Social Security Number
Q5_16) Preferred Bank or Financial Institution
Q5_17) Birthdate
Q5_18) Year of Graduation

Q6: **Debriefing Questions**

Q6_1) Where did you first learn about this study?
Q6_2) Have you ever talked about this study with anyone else?
Q6_3) What do you think was the purpose of the study?
Q6_4) Did any aspect of the study seem odd or suspicious?
Q6_5) What did you notice about Cornell Campus Connect?
Q6_6) What did you notice about Cornell Campus Connect's banner?

Q7: Demographics

Q7_1) What is your race? 1=white/anglo/Caucasian/middle eastern, 2=black/African American, 3=Asian, 4=American indian or Alaskan native, 5=Hispanic or of latino origin, 6=other (Q66_TEXT)
Q7_2) In what year were you born? (text)
Q7_3) What is your gender? 1=male, 2=female

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies, 4258,* 36-58. doi: 10.1007/11957454_3

Acquisti, A., & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Sciences*, *106*, 10975-10980. doi: 10.1073/pnas.0904891106

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, *49*, 160-174. doi: http://doi.org.10.1509/jmr.09.0215

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, CA.: Brooks/Cole.

Archer, R. L., & Berg, J. H. (1978). Disclosure reciprocity and its limits: A reactance analysis. *Journal of Experimental Social Psychology, 14*, 527-540. http://dx.doi.org/10.1016/0022-1031(78)90047-1

Bargh, J. A. (2006). What have we been priming all these years? On the development, mechanisms, and ecology of nonconscious social behavior. *European Journal of Social Psychology*, *36*, 147-168. doi: 10.1002/ejsp.336

Bargh, J. A., Chen, M., & Burrows, L. (1996). Automaticity of social behavior: Direct effects of trait construct and stereotype activation on action. *Journal of Personality and Social Psychology*, *71*, 230-244. doi: 10.1037/0022-3514.71.2.230

Bateson, M., Nettle, D., & Roberts, G. (2006). Cues of being watched enhance cooperation in a real world setting. *Biology Letters, 2*, 412-414. doi:10.1098/rsbl.2006.0509

Bazarova, N. N. (2012). Public intimacy: Disclosure interpretation and social judgments on Facebook. *Journal of Communication, 62,* 815-832. doi: 10.1111/j.1460-2466.2012.01664.x

Bazarova, N. N., & Choi, Y. H. (2014). Self-Disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, 1-23. doi: 10.1111/jcom.12106

Bazarova, N. N., Taft, J. G., Choi, Y. H., & Cosley, D. (2013). Managing impressions and relationships on Facebook: Self-presentational and relational concerns revealed through the analysis of language style. *Journal of Language and Social Psychology, 32*, 121-141. doi: 10.1177/0261927X12456384

boyd, d. (2010, August 23) Social steganography: Learning to hide in plain sight [Web log post]. Retrieved from http://dmlcentral.net/blog/danah-boyd/social-steganography-learning-hide-plain-sight

boyd, d., & Marwick, A. (2011, September). Social privacy in networked publics: Teens' attitudes, practices, and strategies. In *A Decade in Internet Time*: *Dynamics of the Internet and Society (pp. 1-29).* Symposium conducted at the Oxford Internet Institute, Oxford, England. Abstract retrieved from http://journal.webscience.org/682/

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science*, *4*, 340-347. doi: 10.1177/1948550612455931.

Burgoon, J. K., Parrott, R., Le Poire, B. A., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of

relationships. *Journal of Social and Personal Relationships*, *6*, 131-158. doi: 10.1177/026540758900600201

Cesario, J., Plaks, J. E., Hagiwara, N., Navarette, C. D., & Higgins, E. T. (2010). The ecology of automaticity: How situational contingencies shape action semantics and social behavior. *Psychological Science, 21*, 1311-1317. doi: 10.1177/0956797610378685

Chaikin, A. L., & Derlega, V. J. (1974). Variables affecting the appropriateness of self-disclosure. *Journal of Consulting and Clinical Psychology*, *42*, 588-593. doi: 10.1037/h0036614

Chen, B., & Marcus, J. (2012). Students' self-presentation on Facebook: An examination of personality and self-construal factors. *Computers in Human Behavior*, *28*, 2091-2099. doi: 10.1016/j.chb.2012.06.013

Christofides, E., Muise, A., & Desmarais, S. (2011). Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults. *Social Psychological and Personality Science*, *3*, 48-54. doi: 10.1177/1984550611408619

Cohen, J. (2013). *A critical overview of the privacy debates regarding Facebook and an assessment of the" Anti-Facebook" social network, Diaspora** (Doctoral dissertation).

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In *Privacy Online* (pp. 47-60). Springer Berlin Heidelberg.

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15,* 83-108. doi: 10.1111/j.1083-6101.2009.01494.x

Derlega, V. J., & Chaikin, A. L. (2010). Privacy and self-disclosure in social relationships. *Journal of Social Issues, 33,* 102-115. doi: 10.1111/j.1540-4560.1977.tb01885.x

Dijksterhuis, A., & Bargh, J. A. (2001). The perception-behavior expressway: Automatic effects of social perception on social behavior. *Advances in Experimental Social Psychology*, *33*, 1-40. doi: 10.1016/S0065-2601(01)80003-4

Duggan, M. & Brenner, J. (2013). *The demographics of social media users*. In Pew Research Center. Retrieved from http://www.pewinternet.org/2013/02/14/the-demographics-of-social-media-users-2012/

boyd, d. & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer Mediated Communication*, *13*, 210-230. doi: 10.111.j.1083-6101.2007.00393.x

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society*, *13*, 873-892. doi: 10.1177/1461444810385389

Ellison, N. B., Hancock, J. T., & Toma, C. L. (2012). Profile as promise: A framework for conceptualizing veracity in online dating self-presentations. *New Media & Society*, *14*, 45-62. doi: 10.1177/1461444811410395

Ernest-Jones, M., Nettle, D., & Bateson, M. (2011). Effects of eye images on everyday cooperative behavior: A field experiment. *Evolution and Human Behavior, 32,* 172-178. doi: 10.1016/j-evol.humanbehav2010.10.1006

Ferguson, M. J., & Bargh, J. A. (2004). How social perception can automatically influence behavior. *Trends in Cognitive Sciences*, *8*, 33-39. doi: 10.1016/j.tcis.2003.11.004

Fuchs, C. (2012). The political economy of privacy on Facebook. *Television & New Media*, *13*,

139-159. doi: 10.1177/1527476411415699

Greene, K., Derlega, V. J., & Mathews, A. (2006). Self-disclosure in personal relationships. In A. L. Vangelisti & D. Perlman *The Cambridge handbook of personal relationships*, 409-427. New York, NY, US: Cambridge University Press.

Govani, T., & Pashley, H. (2005). *Student awareness of the privacy implications when using Facebook*. Paper presented at the Privacy Poster Fair at the Carnegie Mellon University School of Library and Information Science, Pittsburgh, PA.

Grimmelmann, J. (2008). Saving Facebook. *Iowa Law Review*, *94*, 1137-1206. Retrieved from http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2415&context=fa_pubs

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. ACM Workshop on Privacy in the Electronic Society, Alexandria, VA.

Haley, K. J., & Fessler, D. T. (2005). Nobody's watching? Subtle cues affect generosity in an anonymous economic game. *Evolution & Human Behavior, 26*, 245-256. doi:10.1016/j.evolhumbehav.2005.01.002

Hall, J. A., & Pennington, N. (2013). Self-monitoring, honesty, and cue use on Facebook: The relationship with user extraversion and conscientiousness. *Computers in Human Behavior*, *29*, 1556-1564. doi: 10.1016/j.chb.2013.01.001.

Hancock, J. T., & Toma, C. L. (2009). Putting your best face forward: The accuracy of online dating photographs. *Journal of Communication*, *59*, 367-386. doi: 10.1111/j.1460-2466.2009.01420.x

Heeney, C. (2012). Breaching the contract? Privacy and the UK Census. *The Information Society*, *28*(5), 316-328

Hogan, B. (2010). The presentation of self in the age of social media: Distinguishing performances and exhibitions online. *Bulletin of Science, Technology & Society, 30*, 377-386. doi:10.1177/0270467610385893

Hong, S., Tandoc, E., Kim, E. A., Kim, B., & Wise, K. (2012). The real you? The role of visual cues and comment congruence in perceptions of social attractiveness from Facebook profiles. *Cyberpsychology, Behavior, & Social Networking, 15,* 339-244. doi: 10.1089/cyber.2011.0511

Hooper, V., & Kalidas, T. (2012). Acceptable and unacceptable behaviour on social networking sites: A study of the behavioural norms of youth on Facebook. *Electronic Journal of Information Systems Evaluation*, *15,* 259-268. Retrieved from http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=5b43fe97-7c0c-4023-92ad-567a9db0931d%40sessionmgr4001&vid=1&hid=4209

Jang, S. A. (2012). Self-monitoring as a moderator between descriptive norms and drinking: Findings among Korean and American university students. *Health Communication*, *27*, 546-558. doi: 10.1080/10410236.2011.617242

Joinson, A. N. (2008). Looking at, looking up or keeping up with people?: motives and use of Facebook. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 1027-1036. doi: 10.1145/1357054.1357213

Lampe, C., Ellison, N., & Steinfield, C. (2006). A Face (book) in the crowd: Social searching vs. social browsing. *Proceedings of the 2006 20th Anniversary Conference on Computer Supported Cooperative Work*, 167-170. doi: 10.1145/1180875.1180901

Lampe, C., Ellison, N., & Steinfield, C. (2007). A familiar Face(book): Profile elements

as signals in an online social network. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 435–444. doi: 10.1145/1240624.1240695

Lee, D. (2012, October 5). Facebook surpasses one billion users as it tempts new markets. *BBC News.* Retrieved from http://www.bbc.com/news/technology-19816709

Lennox, R. D., & Wolfe, R. N. (1984). Revision of the self-monitoring scale. *Journal of Personality and Social Psychology, 46,* 1349-1364. doi: 10.1037/0022-3514.46.6.1349.

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A., & Christakis, N. (2008). Tastes, ties, and time: A new social network dataset using Facebook.com. *Social Networks*, *30*, 330-342. doi: 10.1016/j.socnet.2008.07.002

Litt, E., Spottswood, E. L., Birnholtz, J. P., Hancock, J. T., Smith, M. E., & Reynolds, L. (2014). Awkward encounters of an "other" kind: Collective self-presentation and face threat on Facebook. *Proceedings of the ACM Conference on Computer Supported Cooperative Work*, 449-460. doi: 10.1145/2531602.2531646

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference,* 61-70. doi: 10.1145/2068816.2068823

Loersch, C. & Payne, B. K. (2011). The situated inference model: An integrative account of the effects of primes on perception, behavior, and motivation. *Perspectives on Psychological Science, 6*, 234-252. doi: 10.1177/1745691611406921

Madden, M. (2012). *Privacy management on social media sites*. Retrieved from Pew Research Center, Pew Internet and American Life Project site: http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M.

(2013). *Teens, social media, and privacy.* Retrieved from Pew Research Center, Pew Internet and American Life Project site: http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy.pdf

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, *33*, 5-21. Doi: 10.111/j.15440-4650.1977.tb01879.x

Marwick, A. E., & boyd, d. (2011). I tweet honestly, I tweet passionately; Twitter users, context collapse, and the imagined audience. *New Media & Society, 13,* 114-133. doi: 10.1177/1461444810365313

McLaughlin, C., & Vitak, J. (2012). Norm evolution and violation on Facebook. *New Media & Society*, *14*, 299-315. doi: 10.1177/1461444811412712

Metzger, M. J. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal or Computer Mediated Communication, 9.* doi: 10.1111/j.1083-6101.2004.tb00292

Nettle, D., Harper, Z., Kidson, A., Stone, R., Penton-Voak, I.S., and Bateson, M. (2013). The watching eyes effect in the dictator game: It's not how much you give, it's being seen to give something. *Evolution and Human Behavior*, *34,* 35-40. doi: 10.1016/j.evolhumanbehav.2012.08.00

Nettle, D., Nott, K., & Bateson, M. (2012). 'Cycle thieves, we are watching you': Impact of a simple signage intervention against bicycle theft. *PLoS ONE, 7,* 1-5. doi:10.1371/journal.pone.0051738

Newman, M. W., Lauterbach, D., Munson, S. A., Resnick, P., & Morris, M. E. (2011). It's not that I don't have problems, I'm just not putting them on Facebook: Challenges and

opportunities in using online social networks for health. *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*, 341-350. doi: 10.1145/1958824.1958876

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford, CA: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*, 32-48. doi: 10.1162/DAED_a_00113

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. *Computers in Human Behavior*, *26*, 406-418. doi: 10.1016/j.chb.2009.11.012

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte and L. Reinecke (Eds.), *Privacy Online* (pp. 75-89). Berlin: Springer-Verlag.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 40,* 215-236. doi: 10.1177/0093650211418338

Petronio, S. (2002*). Boundaries of privacy: Dialectics of disclosure.* Albany, NY: State University of New York.

Qiu, L., Lin, H., Leung, A. K., & Tov, W. (2012). Putting their best foot forward: Emotional disclosure on Facebook. *Cyberpsychology, Behavior, and Social Networking*, *15*, 569-572. doi: 10.1089/cyber.2012.0200

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*, 1-9. Retrieved from http://dx.doi.org/10.5210/fm.v15i1.2775

Rigdon, M., Ishii, K., Watabe, M., & Kitayama, S. (2009). Minimal social cues in the dictator game. *Journal of Economic Psychology*, *30*, 358-367. doi: 10.1016/.joep.2009.02.002

Rosen, J. (2010, July 21). The web means the end of forgetting. *The New York Times Magazine.* Retrieved from http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html, June 2014.

Smeesters, D., Wheeler, S. C., & Kay, A. C. (2010). Indirect prime-to-behavior effects: The role of perceptions of the self, others, and situations in connecting primed constructs to social behavior. *Advances in Experimental Social Psychology, 42,* 259-317. doi: 10.1016/S0065-2601(10)42005-5

Spottswood, E. L., & Hancock, J. T. (under review). The eyes have it: Eye primes and deceptive behavior on Facebook. *Communication Research.*

Sung, K. T. (2004). Elder respect among young adults: A cross-cultural study of Americans and Koreans. *Journal of Aging Studies*, *18*, 215-230. doi: 10.1016/j.aging.2004.01.002

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. *Computers in Human Behavior*, *27*, 590-598. doi: 10.1016/j.chb.2010.10.017

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*, 7-41. Retrieved from http://repository.cmu.edu/jpc/vol4 /iss2/2

Toma, C. L., Hancock, J. T., & Ellison, N. B. (2008). Separating fact from fiction:

An examination of deceptive self-presentation in online dating profiles. *Personality and Social Psychology Bulletin*, *34*, 1023-1036. doi: 10.1177/0146167208318067

Tufekci, Z. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information, Communication & Society*, *11*, 544-564. doi:10.1080/13691180801999050

Tufekci, Z. (2012). Facebook, youth and privacy in networked publics. *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media*, 338-345. Retrieved from http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/viewFile/4668%26lt%3B/5001

Utz, S., & Krämer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *3*, 1-12. Retrieved from: http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=1

van Dijck, J. (2013). The Culture of Connectivity: A critical history of social media. New York, NY: Oxford University Press.

Waggoner, A. S., Smith, E. R., & Collins, E. C. (2009). Person perception by active verses passive perceivers. *Journal of Experimental Social Psychology, 45,* 1028–1031. doi: 10.1016/j-eso.2009.04.026

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 1-10. doi: 10.1145/2078841

Weisbuch, M., Ivcevic, Z., & Ambady, N. (2009). On being liked on the web and in the "real world": Consistency in first impressions across personal webpages and spontaneous behavior. *Journal of Experimental Social Psychology, 45,* 573–576. doi: 10.1016/j.jesp.2008.12.009

Wheeler, S. C., Smeesters, D., & Kay, A. C. (2011). Culture modifies the operation of prime-to-behavior effects. *Journal of Experimental Social Psychology, 47*, 824- 829. doi: 10.1016/j.jesp.2011.02.018

Wortman, C. B., Adesman, P., Herman, E. & Greenberg, R. (1976). Self-disclosure: An attributional perspective. *Journal of Personality and Social Psychology*, *33*, 184–191. doi: 10.1037/0022-3514.33.2.184

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of Facebook. *Proceedings of the Fourth International Conference on Communities and Technologies*, 265-274. doi: 10.1145/1556460.1556499

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society, 16,* 479-500. doi: 10.1080/1369118X.2013.777757

Table 1

Appropriateness Ratings for the Different Pieces of Information

Information Type	α	*M*	*SD*
Credit Card Information	74.6	1.1	0.39
Social Security Number	88.3	1.16	0.54
Secrets	80.8	1.21	0.49
Medical Information	83.4	1.23	0.54
Banking Information	92.4	1.3	0.75
Home Phone Number	86.6	1.45	0.74
Permanent Address	85.1	1.57	0.76
University ID Number	98.4	1.66	1.05
Location Data	91.0	1.68	0.92
Relationship History	96.2	1.85	1.1
Embarrassing Pictures of You and your Friends	94.4	1.86	1.13
Direct/Private Messages	97.9	1.89	1.35
GPA	90.3	1.93	1.04
Current Address	94.2	1.93	1
Emotional Status Updates	90.3	2.05	1.04
Cell Phone Number	95.2	2.11	1.13
Pictures of you at parties	95.6	2.23	1.19
Academic Standing	93.4	2.3	1.11

Dorm/Off-Campus Housing Area	83.6	2.63	1
Pictures of family	93.4	2.77	1.14
Relationship Status	93.4	2.89	1.11
Academic Accomplishments	86.1	3.02	1.03
University Net ID	97.9	3.11	1.63
Pictures you're tagged in	94.5	3.13	1.2
Email Address	94.4	3.3	1.24
Sexual Orientation	90.6	3.42	1.38
Pictures of Friends	82.7	3.5	0.91
List of your friends	95.9	3.57	1.22
Middle Name	96.5	3.75	1.36
Birth date	93.2	3.83	1.25
Educational Networks	91.7	3.9	1
Hometown	85.9	3.96	1.02
Fraternity/Sorority	82.5	4.06	0.93
Likes/Interests	87.9	4.09	1
Athletic Accomplishments	84.4	4.1	0.94
Classes Taken	93.1	4.26	1.05
Extracurricular activities	91.9	4.34	0.88
Clubs/Organizations	84.9	4.37	0.83
Major	90.2	4.46	0.84
College Affiliation	86.7	4.55	0.81
Graduation Year	94.8	4.62	0.86

Table 2

Mean Differences Between Appropriate, Somewhat Appropriate, and Inappropriate Information Groups

Appropriateness Level	*M*	*SD*	*95% CI Lower*	*95%CI Upper*
Appropriate	4.41	0.12	4.17	4.65
Somewhat Appropriate	2.91	0.10	2.71	3.11
Inappropriate	1.44	0.07	1.29	1.59

Table 3

Items by Information Appropriateness Level

Inappropriate	Somewhat Appropriate	Appropriate
Social Security Number	Phone Number	Hometown
Past Medical Information	Dorm/Off-Campus Housing Area	Club/Student Organization Membership
Preferred Bank or Financial Institution	Relationship Status	Academic Major or Field
University ID Number	Academic Accomplishments	School College Affiliation
Number of Past Romantic Relationships	University Net Id	Year of Graduation
	Email Address	
	Birthdate	
	Likes/Interests	

Table 4

How Frequently and Accurately Participants Disclosed Information in Study 2

	Appropriate		Somewhat		Inappropriate	
	M	*SD*	*M*	*SD*	*M*	*SD*
Frequency	79.8%	0.25	44.4%	0.26	20.1%	0.23
Accuracy	4.29	0.94	3.66	1.31	2.99	1.56

Table 5

Effect of Eyes on Participants' Ability to Correctly Answer Direct versus Indirect Mechanism Questions in Study 2

	Detail		Low Norm		High Norm	
	M	*SE*	*M*	*SE*	*M*	*SE*
Eyes	3.57	0.06	3.95	0.17	3.47	0.18
Control	3.67	0.05	3.78	0.16	3.43	0.15

Table 6

How Frequently and Accurately Participants Disclosed Information in Study 3

	Appropriate		Somewhat		Inappropriate	
	M	*SD*	*M*	*SD*	*M*	*SD*
Frequency	75.3%	0.31	56.3%	0.34	29.8%	0.27
Accuracy	4.11	1.14	3.56	1.29	2.92	1.40

Table 7

Effect of Eyes on Participants' Ability to Correctly Answer Direct versus Indirect Mechanism Questions in Study 3

	Detail		Low Norm		High Norm	
	M	*SE*	*M*	*SE*	*M*	*SE*
Eyes	6.33	0.34	2.36	0.35	1.94	0.33
Control	6.23	0.38	1.93	0.36	1.67	0.30

Figure 1

Effect of No, Low, and High Disclosure Frequency Cues and Eye Primes on Disclosure Frequency in Study 2

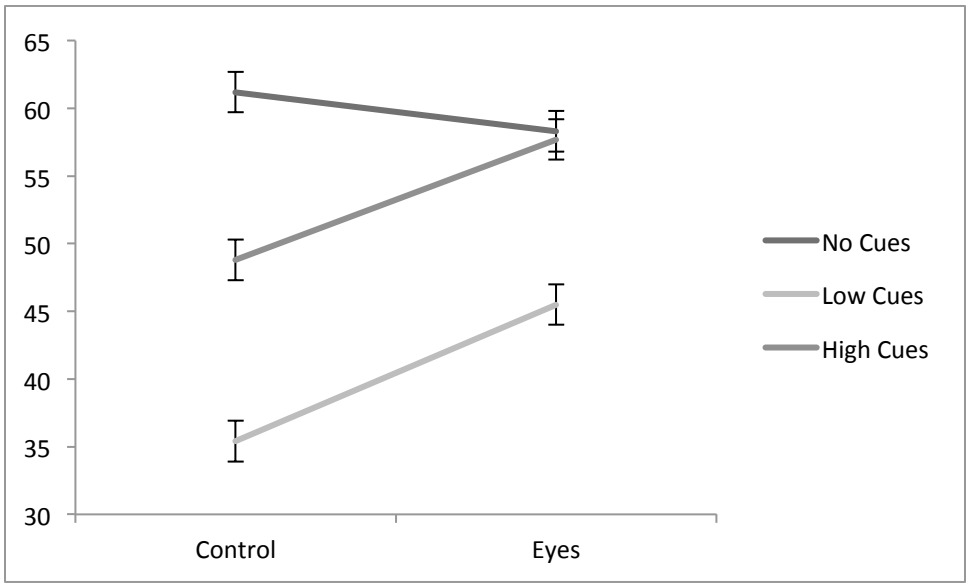


Figure 2

Effect of No, Low, and High Disclosure Frequency Cues and Eye Primes on Disclosure Accuracy in Study 2

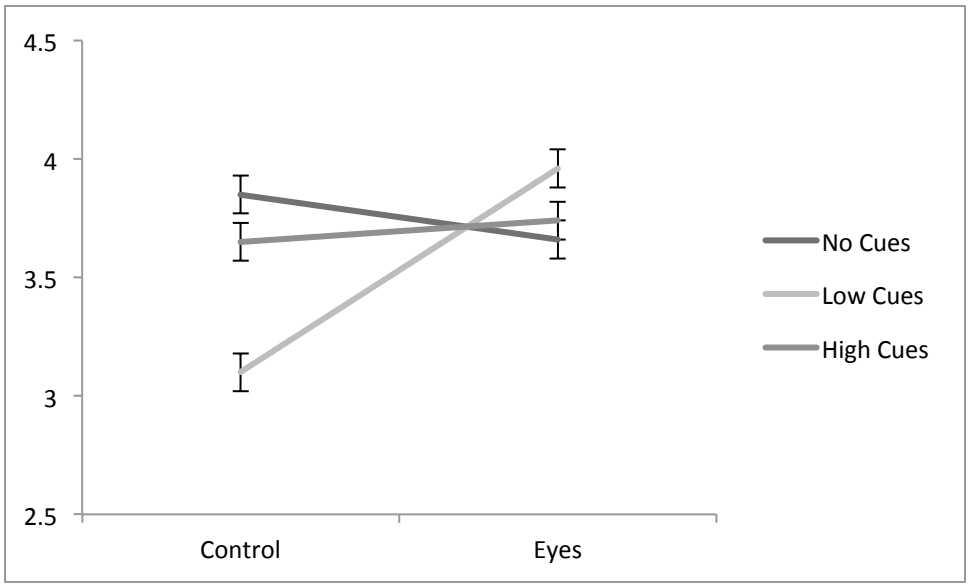


Figure 3

Effect of No, Strict, and Open Privacy Setting Cues and Eye Primes on Privacy Setting Decisions